ESET FILE SECURITY

PER MICROSOFT WINDOWS SERVER

Manuale di installazione e dell'utente

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Fare clic qui per scaricare la versione più recente di questo documento

ESET **FILE SECURITY**

Copyright ©2013 **di ESET, spol. s r.o.**
ESET File Security è stato sviluppato da ESET, spol. s r.o.

Per ulteriori informazioni, visitare il sito Web www.eset.com.
Tutti i diritti riservati. Sono vietate la riproduzione, l'archiviazione in sistemi di registrazione o la trasmissione in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro della presente documentazione in assenza di autorizzazione scritta dell'autore.
ESET, spol. s r.o. si riserva il diritto di modificare qualsiasi parte dell'applicazione software descritta senza alcun preavviso.

Supporto tecnico: www.eset.com/support

REV. 11/11/2013

Contenuti

1. Introduzione....5

1.1 Requisiti di sistema....5

1.2 Tipi di protezione....5

1.3 Interfaccia utente....6

2. Installazione....7

2.1 Installazione tipica....7

2.2 Installazione personalizzata....8

2.3 Terminal Server....10

2.4 Aggiornamento a una versione più recente....10

2.5 Controllo del computer su richiesta....11

3. Guida introduttiva....12

3.1 Introduzione all'interfaccia utente....12

3.1.1 Verifica del funzionamento del sistema....13

3.1.2 Cosa fare se il programma non funziona correttamente....14

3.2 Impostazione aggiornamento....15

3.3 Configurazione del server proxy....16

3.4 Protezione delle impostazioni....17

4. Utilizzo di ESET File Security....18

4.1 ESET File Security - Protezione server....18

4.1.1 Esclusioni automatiche....18

4.2 ESET File Security - Protezione computer....18

4.2.1 Protezione antivirus e antispyware....19

4.2.1.1 Protezione file system in tempo reale....19

4.2.1.1.1 Configurazione del controllo....19

4.2.1.1.1.1 Supporti da controllare....20

4.2.1.1.1.2 Controllo al verificarsi di un evento....20

4.2.1.1.1.3 Opzioni avanzate di controllo....20

4.2.1.1.2 Livelli di pulitura....20

4.2.1.1.3 Quando modificare la configurazione della protezione in tempo reale....21

4.2.1.1.4 Controllo della protezione in tempo reale....21

4.2.1.1.5 Cosa fare se la protezione in tempo reale non funziona....21

4.2.1.2 Protezione client di posta....22

4.2.1.2.1 Controllo POP3....22

4.2.1.2.1.1 Compatibilità....23

4.2.1.2.2 Integrazione con client di posta....24

4.2.1.2.2.1 Aggiunta di notifiche al testo dei messaggi e-mail....25

4.2.1.2.3 Eliminazione delle infiltrazioni....25

4.2.1.3 Protezione accesso Web....26

4.2.1.3.1 HTTP, HTTPS....26

4.2.1.3.1.1 Gestione indirizzo....27

4.2.1.3.1.2 Modalità attiva....28

4.2.1.4 Controllo del computer su richiesta....29

4.2.1.4.1 Tipo di controllo....29

4.2.1.4.1.1 Controllo intelligente....30

4.2.1.4.1.2 Controllo personalizzato....30

4.2.1.4.2 Oggetti da controllare....30

4.2.1.4.3 Profili di controllo....31

4.2.1.4.4 Riga di comando....32

4.2.1.5 Prestazioni....34

4.2.1.6 Filtraggio protocolli....34

4.2.1.6.1 SSL....34

4.2.1.6.1.1 Certificati attendibili....35

4.2.1.6.1.2 Certificati esclusi....35

4.2.1.7 Configurazione parametri motore ThreatSense....35

4.2.1.7.1 Configurazione degli oggetti....36

4.2.1.7.2 Opzioni....36

4.2.1.7.3 Pulitura....38

4.2.1.7.4 Estensioni....39

4.2.1.7.5 Limiti....39

4.2.1.7.6 Altro....40

4.2.1.8 Rilevamento di un'infiltrazione....40

4.3 Aggiornamento del programma....41

4.3.1 Impostazione aggiornamento....43

4.3.1.1 Aggiorna profili....44

4.3.1.2 Configurazione aggiornamento avanzata....44

4.3.1.2.1 Modalità di aggiornamento....44

4.3.1.2.2 Server proxy....46

4.3.1.2.3 Connessione alla LAN....48

4.3.1.2.4 Creazione di copie di aggiornamento - Mirror....49

4.3.1.2.4.1 Aggiornamento dal Mirror....50

4.3.1.2.4.2 Risoluzione dei problemi di aggiornamento Mirror....51

4.3.2 Come creare attività di aggiornamento....51

4.4 Pianificazione attività....52

4.4.1 Scopo della pianificazione delle attività....53

4.4.2 Creazione di nuove attività....53

4.5 Quarantena....54

4.5.1 Mettere file in quarantena....54

4.5.2 Ripristino dalla quarantena....55

4.5.3 Invio di file dalla cartella Quarantena....55

4.6 File di rapporto....56

4.6.1 Filtraggio rapporti....57

4.6.2 Trova nel rapporto....58

4.6.3 Manutenzione rapporto....59

4.7 ESET SysInspector....60

4.7.1 Introduzione a ESET SysInspector....60

4.7.1.1 Avvio di ESET SysInspector....60

4.7.2 Interfaccia utente e utilizzo dell'applicazione....61

4.7.2.1 Comandi del programma....61

4.7.2.2 Spostarsi all'interno di ESET SysInspector....62

4.7.2.2.1 Tasti di scelta rapida....63

4.7.2.3 Confronta....65

4.7.3 Parametri della riga di comando....66

4.7.4 Script di servizio....66

4.7.4.1 Generazione dello script di servizio....66

4.7.4.2 Struttura dello script di servizio....67

4.7.4.3 Esecuzione degli script di servizio....69

4.7.5 Domande frequenti....69

4.7.6 ESET SysInspector come componente di ESET File Security....70

4.8 ESET SysRescue....71

4.8.1 Requisiti minimi....71

4.8.2 Come creare un CD di ripristino....72

4.8.3 Selezione delle destinazioni....72

4.8.4 Impostazioni....72

4.8.4.1 Cartelle....72

4.8.4.2 ESET Antivirus....73

4.8.4.3 Impostazioni avanzate....73

4.8.4.4 Protocollo Internet....73

4.8.4.5 Dispositivo USB di avvio....74

4.8.4.6 Masterizza....74

4.8.5 Utilizzo di ESET SysRescue....74

4.8.5.1 Utilizzo di ESET SysRescue....74

4.9 Interfaccia utente....75

4.9.1 Avvisi e notifiche....76

4.9.2 Disattiva l'interfaccia utente su Terminal Server....77

4.10 eShell....78

4.10.1 Utilizzo....79

4.10.2 Comandi....82

4.10.2.1 Contesto - AV....84

4.10.2.2 Contesto - AV DOCUMENT....86

4.10.2.3 Contesto - AV DOCUMENT LIMITS ARCHIVE....87

4.10.2.4 Contesto - AV DOCUMENT LIMITS OBJECTS....88

4.10.2.5 Contesto - AV DOCUMENT OBJECTS....88

4.10.2.6 Contesto - AV DOCUMENT OPTIONS....91

4.10.2.7 Contesto - AV DOCUMENT OTHER 93
4.10.2.8 Contesto - AV EMAIL 93
4.10.2.9 Contesto - AV EMAIL GENERAL 95
4.10.2.10 Contesto - AV EMAIL GENERAL LIMITS ARCHIVE 95
4.10.2.11 Contesto - AV EMAIL GENERAL LIMITS OBJECTS 96
4.10.2.12 Contesto - AV EMAIL GENERAL OBJECTS 97
4.10.2.13 Contesto - AV EMAIL GENERAL OPTIONS 99
4.10.2.14 Contesto - AV EMAIL GENERAL OTHER 101
4.10.2.15 Contesto - AV EMAIL MESSAGE CONVERT 102
4.10.2.16 Contesto - AV EMAIL MODIFY 102
4.10.2.17 Contesto - AV EMAIL MODIFY RECEIVED 102
4.10.2.18 Contesto - AV EMAIL MODIFY SENT 103
4.10.2.19 Contesto - AV EMAIL OEXPRESS/WINMAIL 104
4.10.2.20 Contesto - AV EMAIL OUTLOOK 104
4.10.2.21 Contesto - AV EMAIL OUTLOOK RESCAN 105
4.10.2.22 Contesto - AV EMAIL PROTOCOL POP3 105
4.10.2.23 Contesto - AV EMAIL PROTOCOL POP3S 106
4.10.2.24 Contesto - AV EMAIL RESCAN 108
4.10.2.25 Contesto - AV EMAIL SCAN 108
4.10.2.26 Contesto - AV EMAIL THUNDERBIRD 110
4.10.2.27 Contesto - AV EMAIL WINLIVE 110
4.10.2.28 Contesto - AV LIMITS ARCHIVE 111
4.10.2.29 Contesto - AV LIMITS OBJECTS 111
4.10.2.30 Contesto - AV NETFILTER 112
4.10.2.31 Contesto - AV NETFILTER PROTOCOL SSL 113
4.10.2.32 Contesto - AV NETFILTER PROTOCOL SSL CERTIFICATE 114
4.10.2.33 Contesto - AV OBJECTS 116
4.10.2.34 Contesto - AV OPTIONS 118
4.10.2.35 Contesto - AV OTHER 119
4.10.2.36 Contesto - AV REALTIME 120
4.10.2.37 Contesto - AV REALTIME DISK 121
4.10.2.38 Contesto - AV REALTIME EVENT 122
4.10.2.39 Contesto - AV REALTIME EXECUTABLE 124
4.10.2.40 Contesto - AV REALTIME EXECUTABLE FROMREMOVABLE 124
4.10.2.41 Contesto - AV REALTIME LIMITS ARCHIVE 125
4.10.2.42 Contesto - AV REALTIME LIMITS OBJECTS 125
4.10.2.43 Contesto - AV REALTIME OBJECTS 126
4.10.2.44 Contesto - AV REALTIME ONWRITE 128
4.10.2.45 Contesto - AV REALTIME ONWRITE ARCHIVE 129
4.10.2.46 Contesto - AV REALTIME OPTIONS 130
4.10.2.47 Contesto - AV REALTIME OTHER 131
4.10.2.48 Contesto - AV REALTIME REMOVABLE 132
4.10.2.49 Contesto - AV WEB 132
4.10.2.50 Contesto - AV WEB ADDRESSMGMT 134
4.10.2.51 Contesto - AV WEB LIMITS ARCHIVE 135
4.10.2.52 Contesto - AV WEB LIMITS OBJECTS 136
4.10.2.53 Contesto - AV WEB OBJECTS 137
4.10.2.54 Contesto - AV WEB OPTIONS 139
4.10.2.55 Contesto - AV WEB OPTIONS BROWSERS 141
4.10.2.56 Contesto - AV WEB OTHER 141
4.10.2.57 Contesto - AV WEB PROTOCOL HTTP 142
4.10.2.58 Contesto - AV WEB PROTOCOL HTTPS 143
4.10.2.59 Contesto - GENERAL 143
4.10.2.60 Contesto - GENERAL ACCESS 144
4.10.2.61 Contesto - GENERAL ESHELL 145
4.10.2.62 Contesto - GENERAL ESHELL COLOR 146
4.10.2.63 Contesto - GENERAL ESHELL OUTPUT 154
4.10.2.64 Contesto - GENERAL ESHELL STARTUP 154
4.10.2.65 Contesto - GENERAL ESHELL VIEW 155
4.10.2.66 Contesto - GENERAL PERFORMANCE 158
4.10.2.67 Contesto - GENERAL PROXY 158
4.10.2.68 Contesto - GENERAL QUARANTINE RESCAN 160
4.10.2.69 Contesto - GENERAL REMOTE 160
4.10.2.70 Contesto - GENERAL REMOTE SERVER PRIMARY 161
4.10.2.71 Contesto - GENERAL REMOTE SERVER SECONDARY 162
4.10.2.72 Contesto - GENERAL TS.NET 163
4.10.2.73 Contesto - GENERAL TS.NET STATISTICS 165
4.10.2.74 Contesto - SCANNER 166
4.10.2.75 Contesto - SCANNER LIMITS ARCHIVE 168
4.10.2.76 Contesto - SCANNER LIMITS OBJECTS 168
4.10.2.77 Contesto - SCANNER OBJECTS 169
4.10.2.78 Contesto - SCANNER OPTIONS 171
4.10.2.79 Contesto - SCANNER OTHER 172
4.10.2.80 Contesto - SERVER 174
4.10.2.81 Contesto - TOOLS 174
4.10.2.82 Contesto - TOOLS ACTIVITY 175
4.10.2.83 Contesto - TOOLS LOG 176
4.10.2.84 Contesto - TOOLS LOG CLEANING 179
4.10.2.85 Contesto - TOOLS LOG OPTIMIZE 179
4.10.2.86 Contesto - TOOLS NOTIFICATION 180
4.10.2.87 Contesto - TOOLS NOTIFICATION EMAIL 181
4.10.2.88 Contesto - TOOLS NOTIFICATION MESSAGE 183
4.10.2.89 Contesto - TOOLS NOTIFICATION MESSAGE FORMAT 183
4.10.2.90 Contesto - TOOLS NOTIFICATION WINPOPUP 184
4.10.2.91 Contesto - TOOLS SCHEDULER 185
4.10.2.92 Contesto - TOOLS SCHEDULER EVENT 186
4.10.2.93 Contesto - TOOLS SCHEDULER FAILSAFE 187
4.10.2.94 Contesto - TOOLS SCHEDULER PARAMETERS CHECK 188
4.10.2.95 Contesto - TOOLS SCHEDULER PARAMETERS EXTERNAL 189
4.10.2.96 Contesto - TOOLS SCHEDULER PARAMETERS SCAN 190
4.10.2.97 Contesto - TOOLS SCHEDULER PARAMETERS UPDATE 191
4.10.2.98 Contesto - TOOLS SCHEDULER REPEAT 191
4.10.2.99 Contesto - TOOLS SCHEDULER STARTUP 192
4.10.2.100 Contesto - UPDATE 193
4.10.2.101 Contesto - UPDATE CONNECTION 195
4.10.2.102 Contesto - UPDATE MIRROR 197
4.10.2.103 Contesto - UPDATE MIRROR CONNECTION 199
4.10.2.104 Contesto - UPDATE MIRROR SERVER 200
4.10.2.105 Contesto - UPDATE NOTIFICATION 201
4.10.2.106 Contesto - UPDATE PROXY 202
4.10.2.107 Contesto - UPDATE SYSTEM 203

4.11 Importa ed esporta impostazioni 204

4.12 ThreatSense.Net 205

4.12.1 File sospetti 206
4.12.2 Statistiche 207
4.12.3 Invio 208

4.13 Amministrazione remota 209

4.14 Licenze 210

5. Glossario 211

5.1 Tipi di infiltrazioni 211

5.1.1 Virus 211
5.1.2 Worm 211
5.1.3 Trojan horse 212
5.1.4 Rootkit 212
5.1.5 Adware 212
5.1.6 Spyware 213
5.1.7 Applicazioni potenzialmente pericolose 213
5.1.8 Applicazioni potenzialmente indesiderate 213

1. Introduzione

ESET File Security è una soluzione integrata sviluppata specificatamente per l'ambiente Microsoft Windows Server. ESET File Security assicura una protezione efficace e valida contro vari tipi di malware e offre due tipi di protezione: antivirus e antispyware.

Alcune delle funzionalità principali di ESET File Security:

- Esclusioni automatiche - Rilevamento ed esclusione automatici di file server critici per un utilizzo semplificato.
- eShell (ESET Shell) - Nuova interfaccia di controllo della riga di comando che offre agli utenti avanzati e agli amministratori opzioni più complete per la gestione dei prodotti ESET.
- Autoprotezione - Tecnologia che protegge contro la modifica o la disattivazione delle soluzioni di protezione ESET.
- Risoluzione dei problemi efficace, con strumenti integrati avanzati per la risoluzione di varie problematiche: ESET SysInspector per la diagnostica del sistema ed ESET SysRescue per la creazione di un CD di ripristino di avvio.

ESET File Security supporta le versioni indipendenti di Microsoft Windows Server 2000, 2003 e 2008, oltre a Microsoft Windows Server in un ambiente cluster. ESET Remote Administrator consente la gestione remota di ESET File Security in reti di grandi dimensioni.

1.1 Requisiti di sistema

Sistemi operativi supportati:

- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 e x64)
- Microsoft Windows Server 2008 (x86 e x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Storage Server 2008 R2 Essentials SP1
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

I requisiti hardware dipendono dalla versione del sistema operativo in uso. Per informazioni più dettagliate sui requisiti hardware, si consiglia di consultare la documentazione del prodotto Microsoft Windows Server.

1.2 Tipi di protezione

Esistono due tipi di protezione:

- Protezione antivirus
- Protezione antispyware

La protezione antivirus e antispyware è una delle funzioni di base di ESET File Security. Questo tipo di protezione difende il sistema da attacchi dannosi controllando file, messaggi e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla: prima bloccandola e poi pulendola, eliminandola o mettendola in quarantena.

1.3 Interfaccia utente

ESET File Security dispone di un'interfaccia utente (GUI) progettata per essere il più intuitiva possibile. L'interfaccia offre agli utenti un accesso semplice e rapido alle principali funzioni del programma.

Oltre all'interfaccia utente principale, è disponibile una **struttura di configurazione avanzata** accessibile da qualsiasi schermata del programma premendo il tasto F5.

Quando si preme F5, viene visualizzata la struttura di configurazione avanzata contenente un elenco delle funzionalità del programma configurabili. In questa finestra è possibile configurare le impostazioni e le opzioni preferite. La struttura ad albero è suddivisa in due sezioni: **Protezione server** e **Protezione computer**. Nella sezione **Protezione server** sono contenute le esclusioni automatiche, specifiche per il sistema operativo del server e i file di sistema. Nella sezione **Protezione computer** sono contenuti gli elementi configurabili per la protezione del server.

2. Installazione

Dopo aver acquistato ESET File Security, è possibile scaricare il programma di installazione dal sito Web di ESET (www.eset.com) come pacchetto MSI.

Tenere presente che è necessario eseguire il programma di installazione con l'account **Amministratore incorporato**. Qualsiasi altro utente, pur essendo membro del gruppo Amministratori, non disporrà dei sufficienti diritti di accesso. Sarà pertanto necessario utilizzare l'account Amministratore incorporato poiché non sarà possibile completare correttamente l'installazione con qualsiasi altro account utente diverso da **Amministratore**.

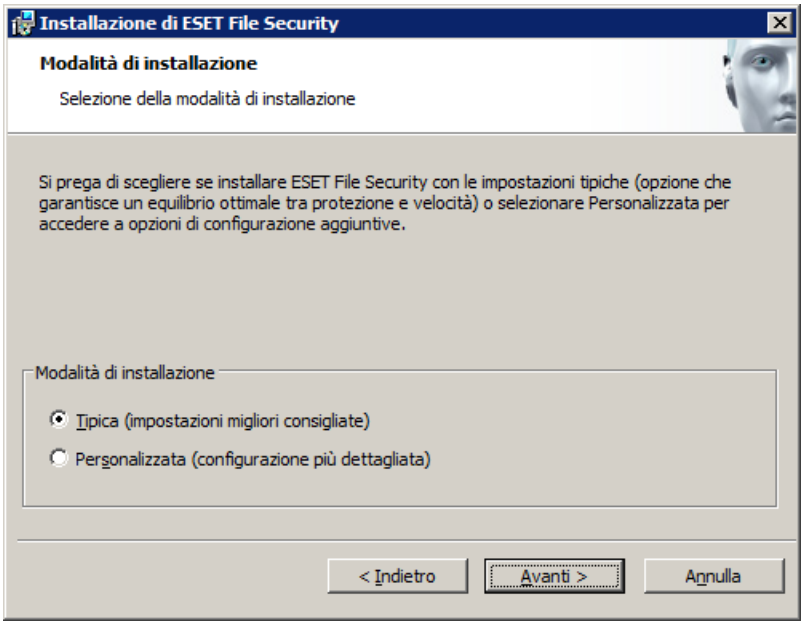
Il programma di installazione può essere eseguito in due modi:

- È possibile eseguire l'accesso a livello locale utilizzando le credenziali dell'account Amministratore ed eseguire semplicemente il programma di installazione
- È possibile eseguire l'accesso come un altro utente ma è necessario aprire il prompt dei comandi con **Esegui come...** e immettere le credenziali dell'account Amministratore affinché il cmd sia eseguito come Amministratore, quindi digitare il comando per l'esecuzione del programma di installazione, ad esempio `msiexec /i efsw_nt64_ENU.msi` ma è necessario sostituire `efsw_nt64_ENU.msi` con il nome esatto del file del programma di installazione MSI scaricato.

Dopo aver avviato il programma di installazione, l'installazione guidata condurrà l'utente attraverso le fasi della configurazione di base. Sono disponibili due tipi di installazione con differenti livelli di dettagli della configurazione:

1. **Installazione tipica**

2. **Installazione personalizzata**


Installazione di ESET File Security
Modalità di installazione
Selezione della modalità di installazione
Si prega di scegliere se installare ESET File Security con le impostazioni tipiche (opzione che garantisce un equilibrio ottimale tra protezione e velocità) o selezionare Personalizzata per accedere a opzioni di configurazione aggiuntive.
Modalità di installazione
Tipica (impostazioni migliori consigliate)
Personalizzata (configurazione più dettagliata)
< Indietro
Avanti >
Annulla

NOTA: è consigliabile installare ESET File Security su un sistema operativo appena installato e configurato, se possibile. Se è tuttavia necessario installarlo su un sistema esiste, è opportuno disinstallare la versione precedente di ESET File Security, riavviare il server e installare successivamente la nuova versione di ESET File Security.

2.1 Installazione tipica

La modalità di installazione tipica consente di installare rapidamente ESET File Security con una configurazione minima durante la procedura di installazione. La modalità di installazione tipica rappresenta l'opzione predefinita consigliata nel caso in cui gli utenti non abbiano particolari necessità relative a impostazioni specifiche. Dopo aver installato ESET File Security sul sistema, in qualsiasi momento è possibile modificare le opzioni e le impostazioni di configurazione. In questo manuale dell'utente vengono descritte in dettaglio tali impostazioni e funzionalità. Le impostazioni della modalità di installazione tipica assicurano protezione ottimale, facilità di utilizzo e prestazioni elevate del sistema.

Dopo aver scelto la modalità di installazione e aver selezionato Avanti, all'utente verrà richiesto di immettere il nome utente e la password. Questa operazione è essenziale per garantire una protezione costante al sistema poiché il nome utente e la password consentono Aggiornamenti del database delle firme antivirali.

Immettere il nome utente e la password ricevuti dopo aver acquistato o registrato il prodotto nei rispettivi campi. Nel caso in cui non si disponga attualmente di nome utente e password, potranno essere inseriti successivamente direttamente dal programma.

Nel passaggio successivo, **Gestione licenze**, aggiungere il file di licenza ricevuto tramite e-mail dopo aver acquistato il prodotto.

La fase successiva consiste nella configurazione del Sistema di allarme immediato ThreatSense.Net. Il Sistema di allarme immediato ThreatSense.Net consente di garantire che ESET sia informata in modo tempestivo e continuativo sulle nuove infiltrazioni per proteggere gli utenti in modo immediato. Il sistema consente l'invio di nuove minacce ai laboratori antivirus ESET, dove i virus verranno analizzati, elaborati e aggiunti al database delle firme antivirali. Per impostazione predefinita, l'opzione **Attiva Sistema di allarme immediato ThreatSense.Net** è selezionata. Fare clic su **Configurazione avanzata...** per modificare le impostazioni dettagliate sull'invio dei file sospetti.

Il passaggio successivo del processo di installazione consiste nella configurazione del **Rilevamento delle applicazioni potenzialmente indesiderate**. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Per ulteriori informazioni, consultare il capitolo Applicazioni potenzialmente indesiderate.

Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile rilevarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

Selezionare l'opzione **Attiva rilevamento delle applicazioni potenzialmente indesiderate** per consentire a ESET File Security di rilevare questo tipo di applicazioni. Se non si desidera utilizzare questa funzionalità, selezionare **Disattiva rilevamento delle applicazioni potenzialmente indesiderate.**

L'ultimo passaggio della modalità di installazione tipica consiste nella conferma dell'installazione mediante il pulsante **Installa**.

2.2 Installazione personalizzata

L'installazione personalizzata è adatta agli utenti che desiderano configurare ESET File Security durante la procedura di installazione.

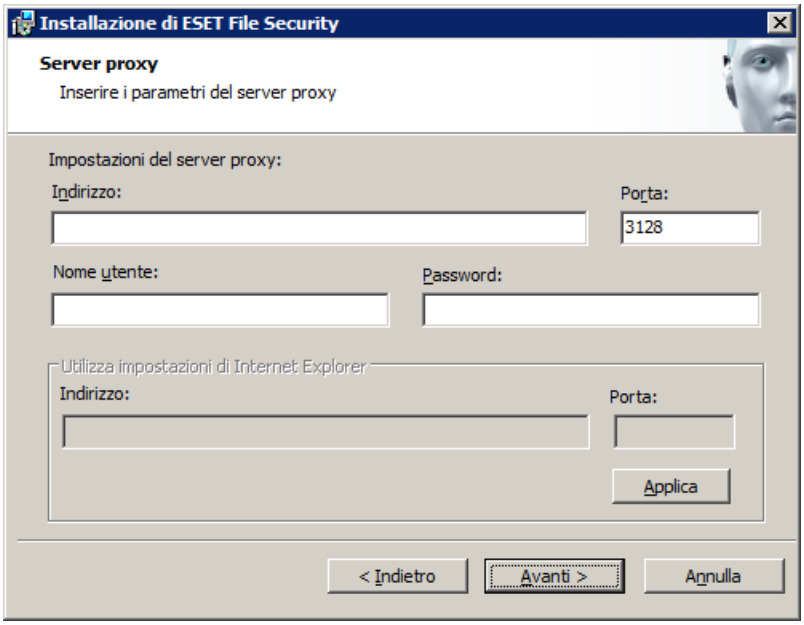
Dopo aver selezionato la modalità di installazione e aver selezionato **Avanti**, verrà chiesto di selezionare un percorso di destinazione per l'installazione. Per impostazione predefinita, il programma viene installato nel percorso *C:\Programmi\ESET\ESET File Security*. Fare clic su **Sfoglia...** per selezionare un percorso diverso (scelta non consigliata).

Quindi, immettere il **Nome utente** e **Password**. Questo passaggio è analogo a quello dell'Installazione tipica (consultare "Installazione tipica").

Nel passaggio successivo, **Gestione licenze**, aggiungere il file di licenza ricevuto tramite e-mail dopo aver acquistato il prodotto.

Dopo aver inserito il nome utente e la password, fare clic su **Avanti** per passare a **Configura connessione Internet**.

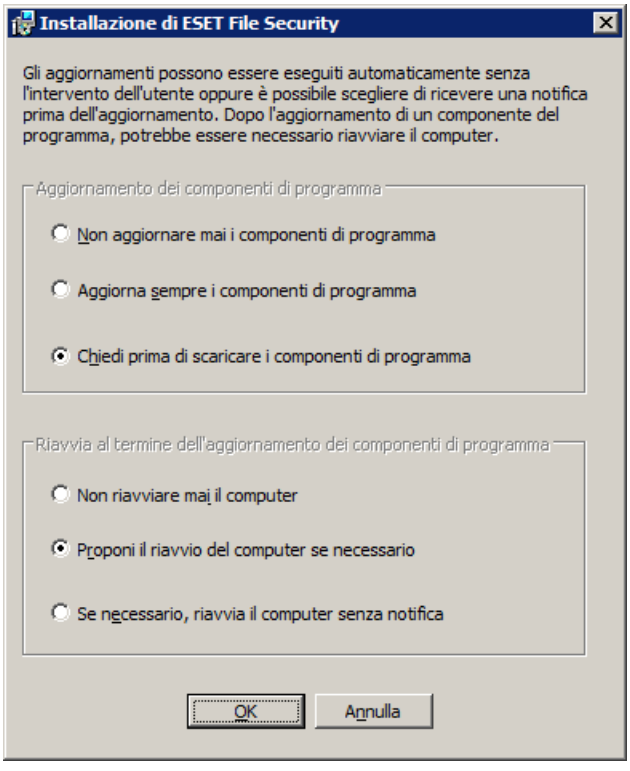
Se si utilizza un server proxy, è necessario configurarlo correttamente per l'esecuzione degli aggiornamenti delle firme antivirali. Se si desidera che il server proxy sia configurato automaticamente, selezionare l'impostazione predefinita **Utilizzare le stesse impostazioni di Internet Explorer poiché non è certo che venga utilizzato un server proxy per la connessione Internet (scelta consigliata)** e fare clic su **Avanti**. Se non si utilizza un server proxy, selezionare l'opzione **Non viene utilizzato un server proxy**.



Se si preferisce immettere i dettagli del server proxy, è possibile configurare manualmente le relative impostazioni. Per configurare le impostazioni del server proxy, selezionare **Viene utilizzato un server proxy**, quindi fare clic su **Avanti**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo**. Nel campo **Porta** specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Nel caso in cui il server proxy richieda l'autenticazione, sarà necessario immettere un **Nome utente** e **Password** validi per consentire l'accesso al server proxy. Se si desidera è anche possibile copiare le impostazioni del server proxy da Internet Explorer. Dopo aver immesso i dettagli del server proxy, fare clic su **Applica** e confermare la selezione.

Fare clic su **Avanti** per passare a **Configura impostazioni aggiornamento** automatico. In questa fase è possibile specificare la modalità di gestione degli aggiornamenti automatici dei componenti di programma sul sistema. Scegliere **Cambia...** per accedere alle impostazioni avanzate.

Se non si desidera aggiornare i componenti di programma, selezionare l'opzione **Non aggiornare mai i componenti di programma**. Selezionare l'opzione **Chiedi prima di scaricare componenti di programma** per visualizzare una finestra di conferma prima di scaricare i componenti di programma. Per scaricare automaticamente gli aggiornamenti dei componenti di programma, selezionare l'opzione **Aggiorna sempre i componenti di programma**.


Installazione di ESET File Security
Gli aggiornamenti possono essere eseguiti automaticamente senza l'intervento dell'utente oppure è possibile scegliere di ricevere una notifica prima dell'aggiornamento. Dopo l'aggiornamento di un componente del programma, potrebbe essere necessario riavviare il computer.
Aggiornamento dei componenti di programma
Non aggiornare mai i componenti di programma
Aggiorna sempre i componenti di programma
Chiedi prima di scaricare i componenti di programma
Riavvia al termine dell'aggiornamento dei componenti di programma
Non riavviare mai il computer
Proponi il riavvio del computer se necessario
Se necessario, riavvia il computer senza notifica
OK
Annulla

NOTA: in genere, dopo aver aggiornato un componente di programma, è necessario riavviare il sistema. Si consiglia di selezionare l'opzione **Non riavviare mai il computer**. Gli aggiornamenti dei componenti più recenti entreranno

in vigore al successivo riavvio del server (sia esso pianificato, manuale o di altro tipo). Se si desidera ricevere un promemoria per il riavvio del server al termine dell'aggiornamento dei componenti, selezionare l'opzione **Proponi il riavvio del computer se necessario**. Questa impostazione consente di riavviare il server immediatamente oppure di posticipare il riavvio ed eseguirlo successivamente.

Nella finestra di installazione successiva è disponibile l'opzione per impostare una password per proteggere le impostazioni del programma. Selezionare l'opzione **Proteggi le impostazioni di configurazione con password** e scegliere una password da immettere nei campi **Nuova password** e **Conferma nuova password**.

I due successivi passaggi di installazione, **Sistema di allarme immediato ThreatSense.Net** e **Rilevamento di applicazioni potenzialmente indesiderate** sono uguali ai passaggi della modalità di installazione tipica (consultare "Installazione tipica").

Fare clic su **Installa** nella finestra **Pronto all'installazione** per completare l'installazione.

2.3 Terminal Server

Se ESET File Security è stato installato su Windows Server che funge da Terminal Server, potrebbe essere necessario disattivare l'interfaccia utente di ESET File Security per impedire che venga avviata all'accesso di un utente. Per informazioni dettagliate su come disattivarla, consultare il capitolo Disattiva l'interfaccia utente su Terminal Server .

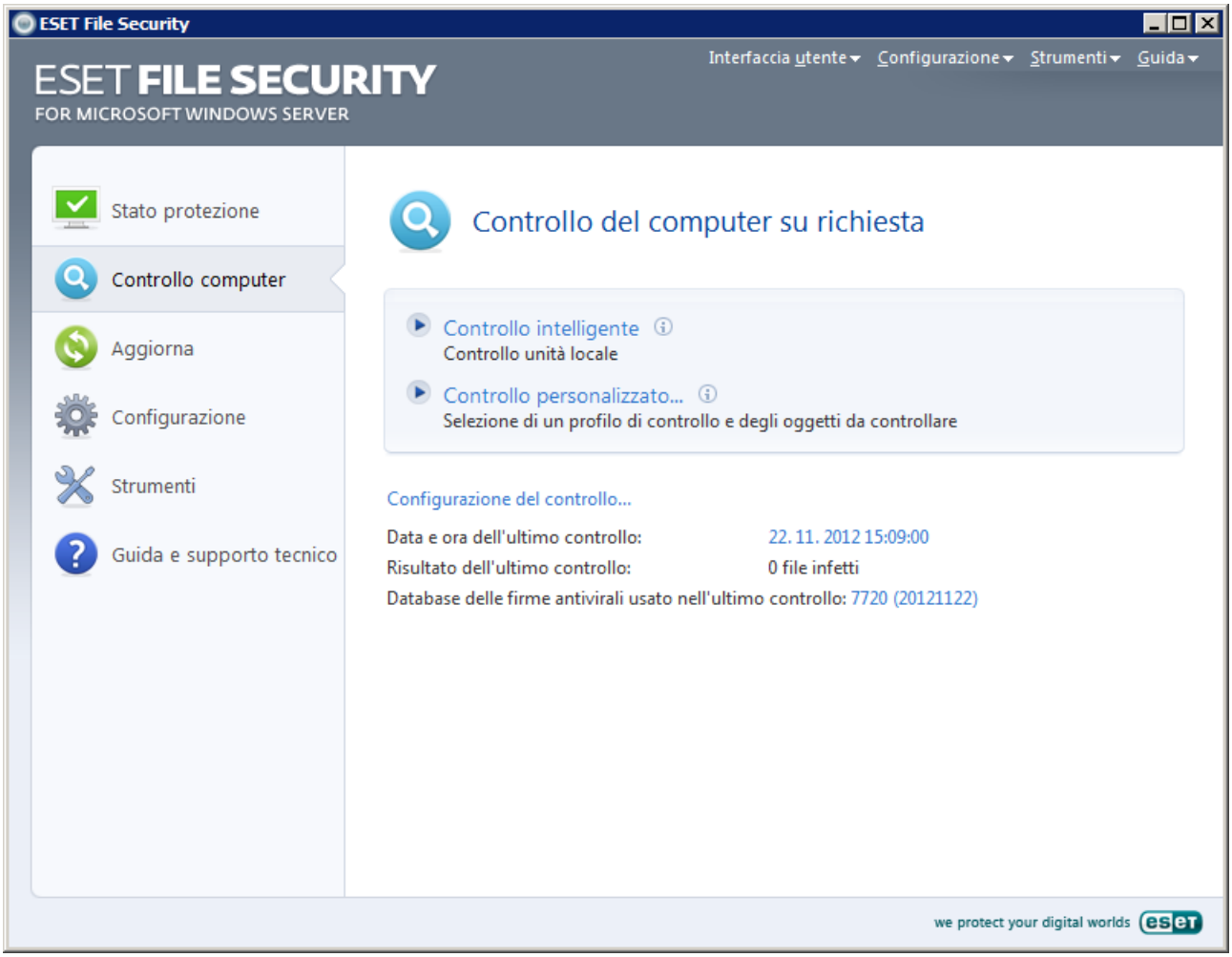
2.4 Aggiornamento a una versione più recente

Versioni più recenti di ESET File Security vengono rilasciate per apportare miglioramenti o correggere problemi che non è possibile risolvere mediante gli aggiornamenti automatici dei moduli del programma. L'aggiornamento a una versione più recente può essere eseguito in diversi modi:

1. Aggiornamento automatico tramite un aggiornamento dei componenti di programma (PCU)
   Poiché gli aggiornamenti dei componenti di programma vengono distribuiti a tutti gli utenti e possono influenzare alcune configurazioni del sistema, vengono rilasciati per un lungo periodo di prova per consentire un processo di aggiornamento lineare su tutte le possibili configurazioni di sistema. Se è necessario eseguire l'aggiornamento a una versione più recente nel momento in cui viene rilasciato, usare uno dei metodi seguenti.
2. Manualmente scaricando e installando una nuova versione su quella precedente
   All'inizio dell'installazione, è possibile scegliere di preservare le impostazioni correnti del programma selezionando la casella di controllo **Utilizza impostazioni correnti**.
3. Manualmente con la distribuzione automatica in un ambiente di rete tramite ESET Remote Administrator.

2.5 Controllo del computer su richiesta

Dopo aver installato ESET File Security, è necessario eseguire un controllo del computer alla ricerca di codici dannosi. Nella finestra principale del programma, fare clic su **Controllo computer**, quindi fare clic su **Controllo intelligente**. Per ulteriori informazioni sui controlli del computer su richiesta, consultare la sezione Controllo del computer su richiesta.



3. Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET File Security e sulle configurazioni di base.

3.1 Introduzione all'interfaccia utente

La finestra principale di ESET File Security è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Di seguito è riportata una descrizione delle opzioni del menu principale:

Stato protezione - Fornisce informazioni relative allo stato di protezione di ESET File Security. Se è attiva la modalità avanzata, sarà visualizzato il sottomenu **Attività di verifica** e **Statistiche**.

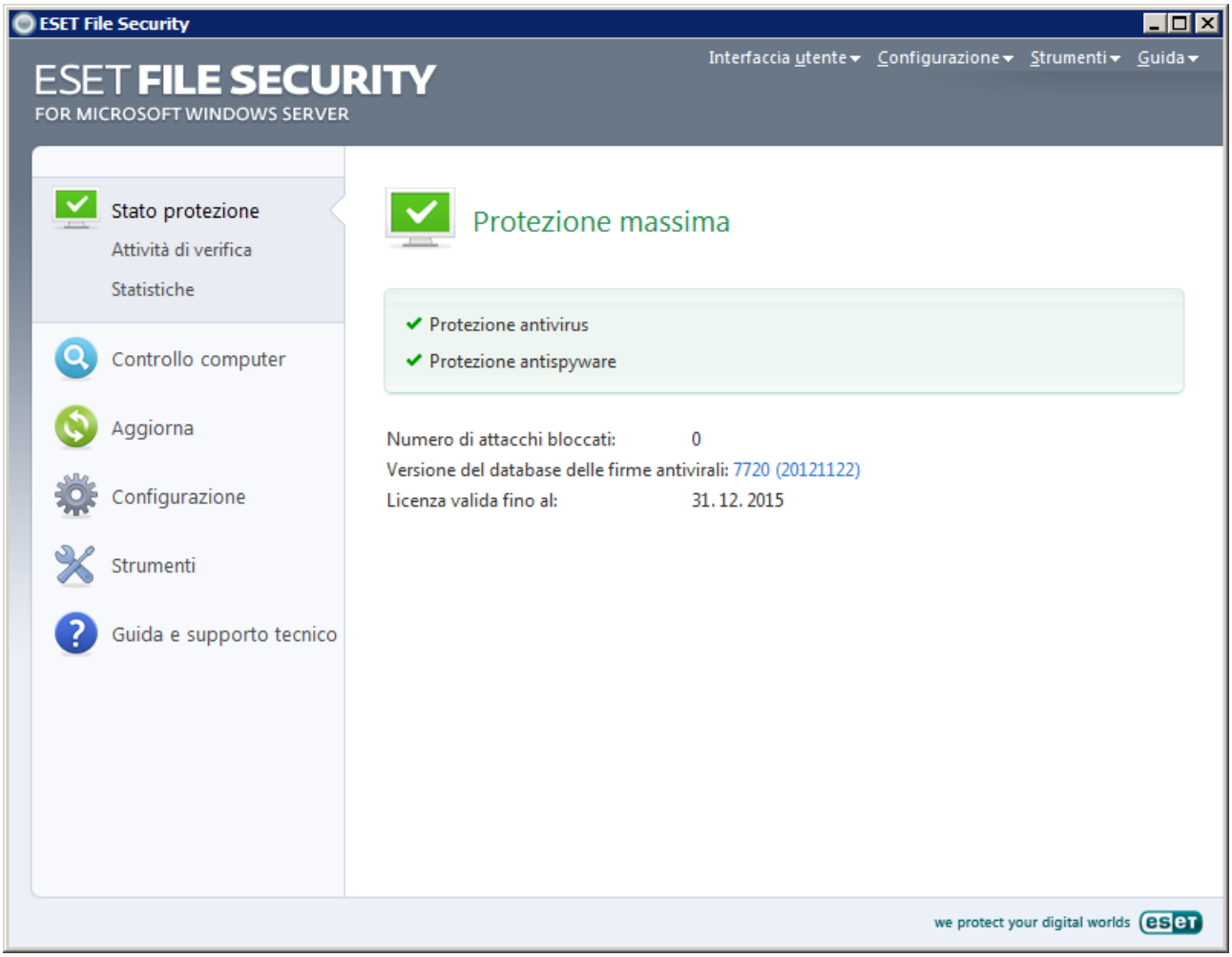
Controllo computer - Questa opzione consente di configurare e avviare un Controllo computer su richiesta.

Aggiorna - Consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.

Configurazione - Selezionare questa opzione per regolare il livello di protezione del computer. Se è attiva la modalità avanzata, sarà visualizzato il sottomenu **Antivirus e antispyware**.

Strumenti - Consente di accedere a **File di rapporto**, **Quarantena**, **Pianificazione attività** e **SysInspector**. Questa opzione viene visualizzata solo nella modalità avanzata.

Guida e supporto tecnico - Consente di accedere ai file della Guida, alla Knowledge Base ESET, al sito Web ESET e ai collegamenti per aprire una richiesta di assistenza al Supporto tecnico.



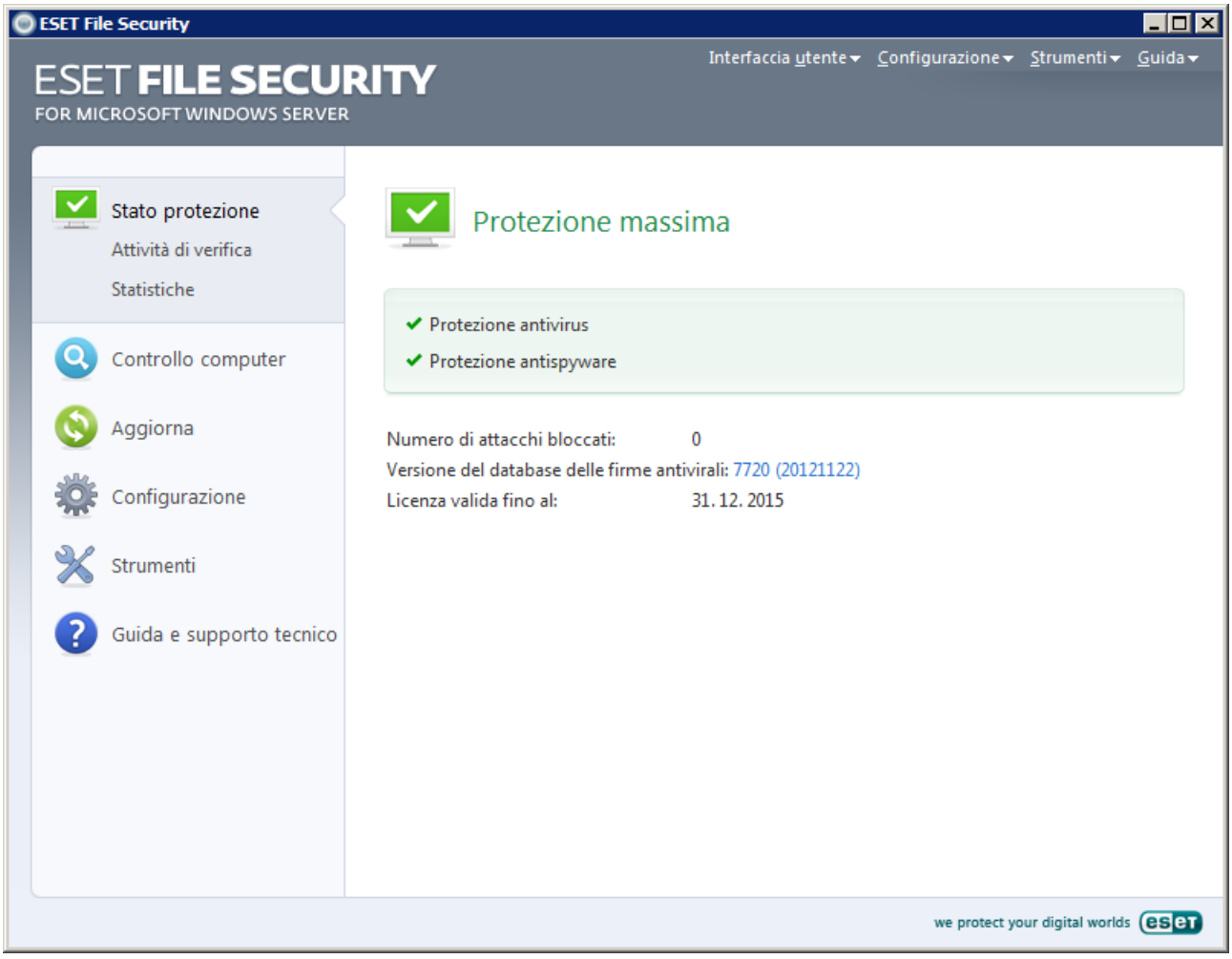
3.1.1 Verifica del funzionamento del sistema

Per visualizzare lo **Stato protezione**, fare clic sulla prima opzione nel menu principale. Nella finestra principale verrà visualizzato un riepilogo sullo stato di funzionamento di ESET File Security. Verrà inoltre visualizzato un sottomenu con due elementi: **Attività di verifica** e **Statistiche**. Selezionare una delle due opzioni per visualizzare informazioni più dettagliate sul sistema.

Se ESET File Security viene eseguito con le funzionalità complete, l'opzione **Stato protezione** appare in verde. In caso contrario, viene visualizzata in arancione o rosso, il che significa che richiede attenzione da parte dell'utente.

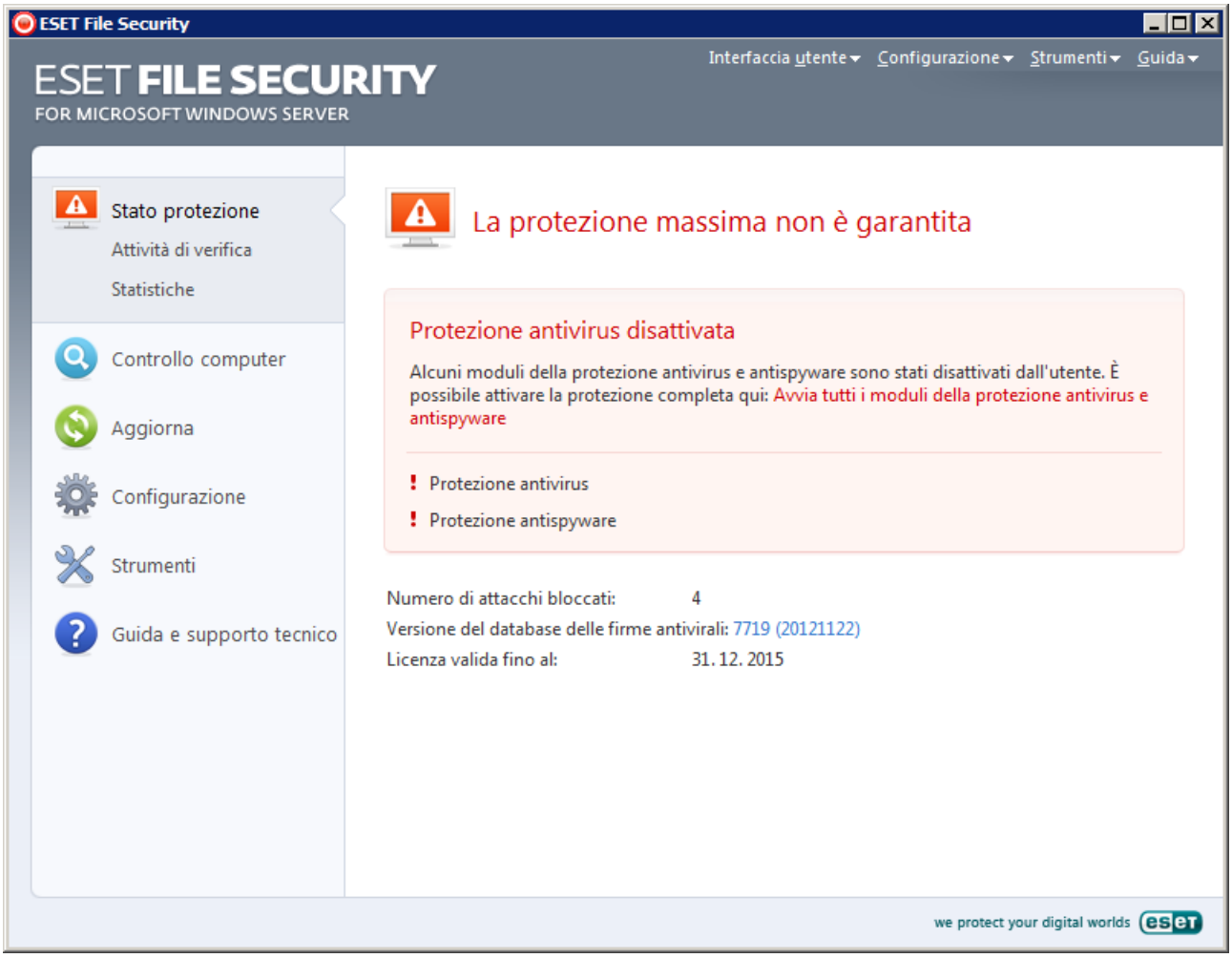
Se si fa clic sulla voce del sottomenu **Attività di verifica**, è possibile visualizzare l'attività corrente del file system sotto forma di grafico in tempo reale (asse orizzontale). Sull'asse verticale viene mostrata la quantità di dati letti (riga blu) e dati scritti (riga rossa).

Il sottomenu **Statistiche** consente di visualizzare il numero di oggetti infettati, puliti e non infetti di un modulo specifico. Nell'elenco a discesa sono disponibili diversi moduli tra i quali scegliere.



3.1.2 Cosa fare se il programma non funziona correttamente

Se i moduli attivati funzionano correttamente, verrà visualizzato un segno di spunta di controllo verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione e, nella parte superiore della finestra, verranno visualizzate ulteriori informazioni sul modulo. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato dei singoli moduli, scegliere **Configurazione** dal menu principale e fare clic sul modulo desiderato.

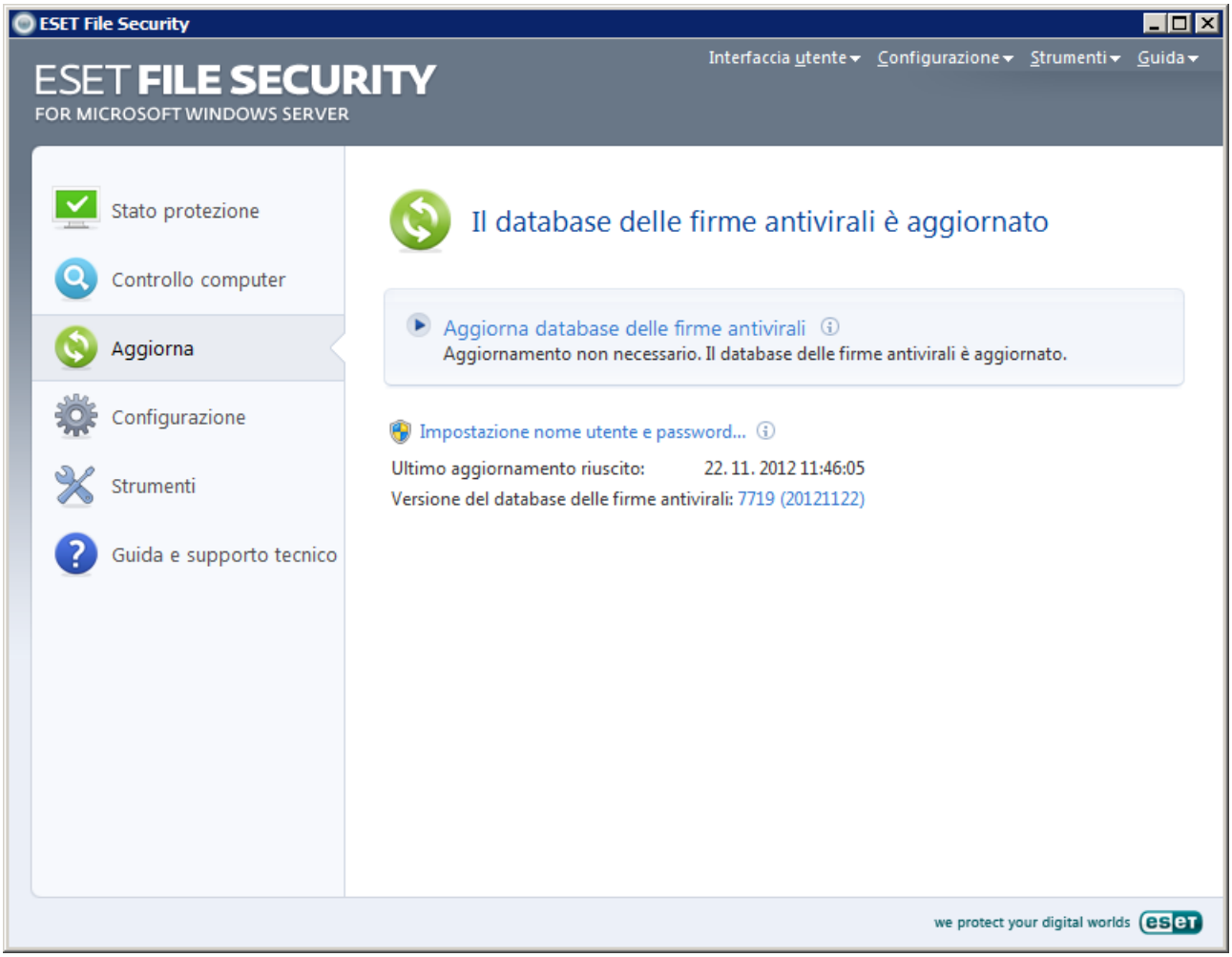


Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su Guida e supporto tecnico per accedere ai file della Guida o effettuare una ricerca nella Knowledge Base. Nel caso in cui sia necessaria assistenza, è possibile inviare una richiesta al Supporto tecnico ESET. Il Supporto tecnico ESET risponderà rapidamente alle domande degli utenti e li aiuterà a ricercare una soluzione ai loro problemi.

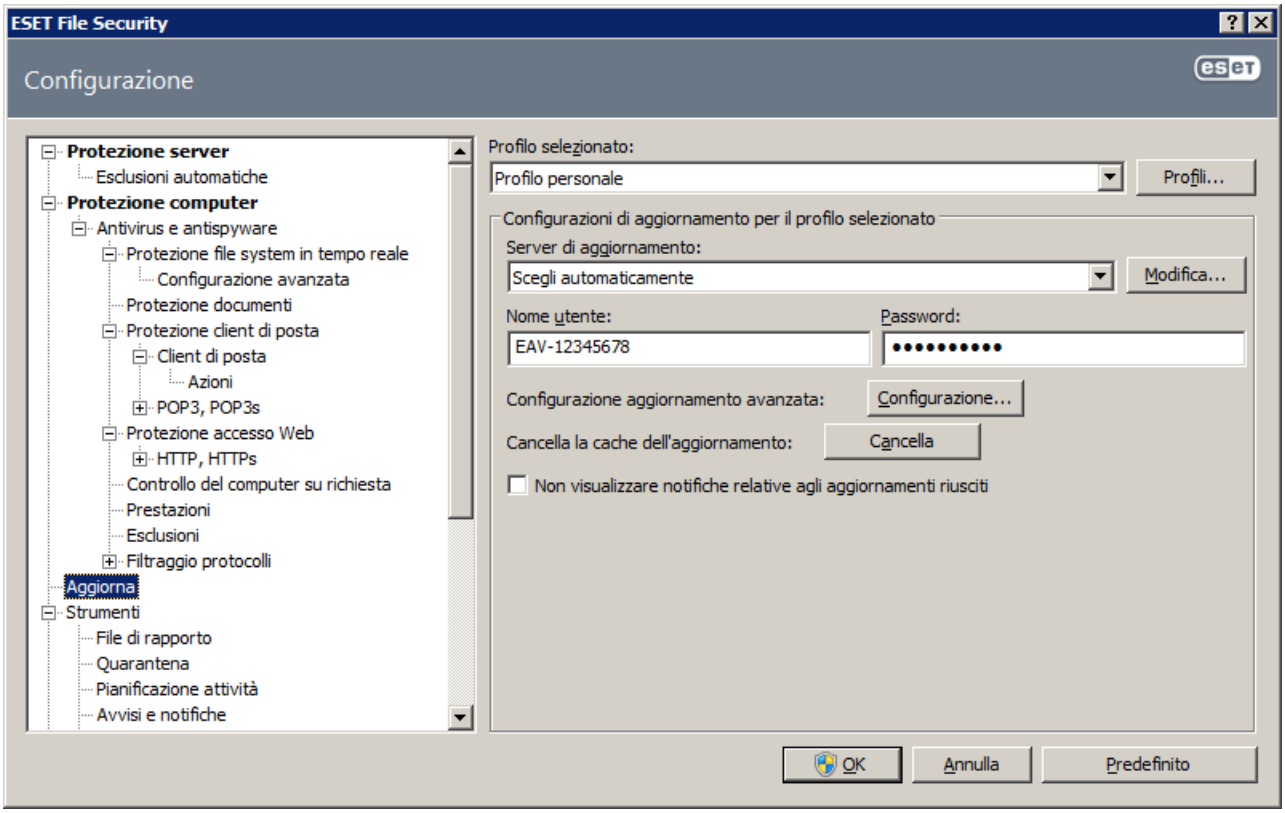
3.2 Impostazione aggiornamento

L'aggiornamento del database delle firme antivirali e dei componenti di programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e funzionamento. Nel menu principale, selezionare **Aggiorna**, quindi fare clic su **Aggiorna database delle firme antivirali** nella finestra principale per verificare la disponibilità di un aggiornamento recente del database. L'opzione **Configurazione nome utente e password...** consente di visualizzare una finestra di dialogo dove immettere il nome utente e la password ricevuti all'acquisto.

Se il nome utente e la password sono stati specificati durante l'installazione di ESET File Security, non verrà richiesto di inserirli ora.

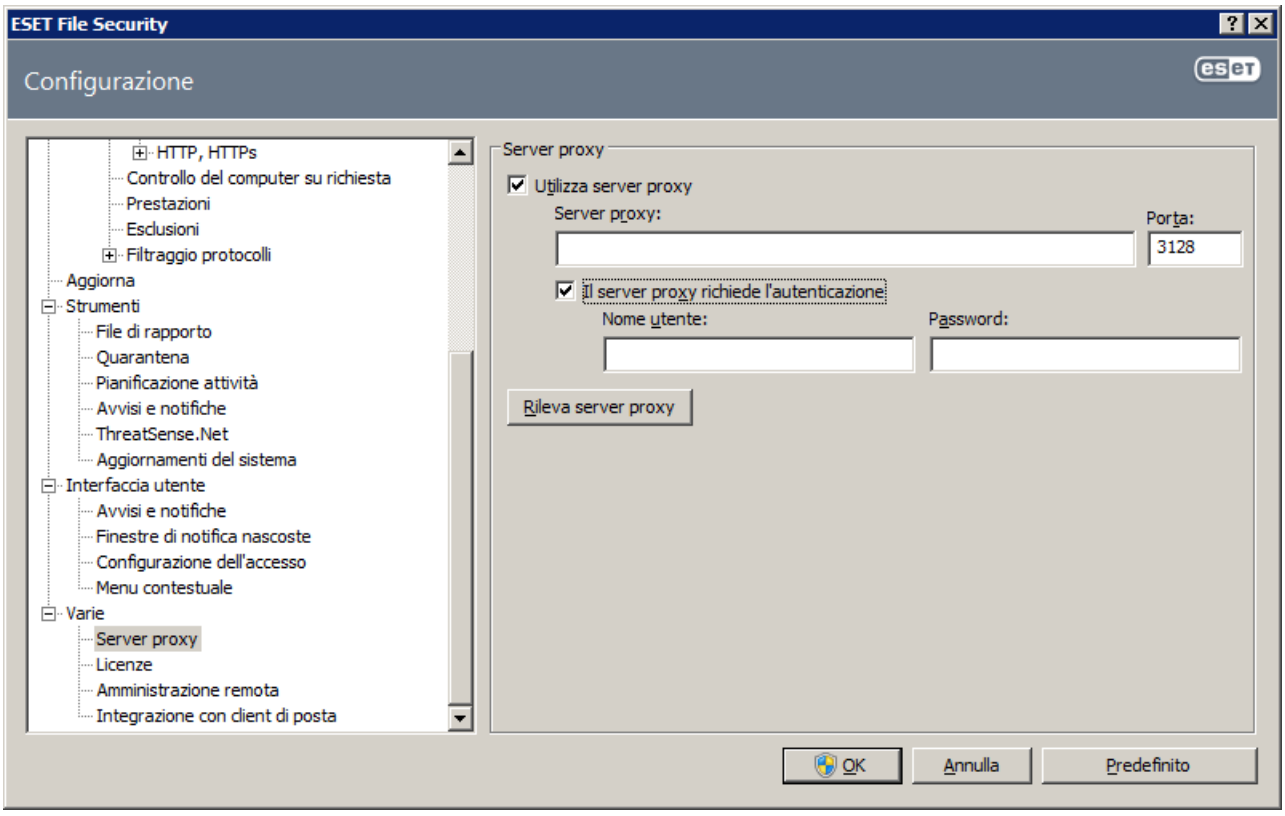


La finestra Configurazione avanzata (fare clic su **Configurazione** dal menu principale, quindi scegliere **Immetti struttura di configurazione avanzata completa...**, oppure premere F5) contiene ulteriori opzioni di aggiornamento. Fare clic su **Aggiorna** nella struttura Configurazione avanzata. Il menu a discesa **Server di aggiornamento**: deve essere configurato su **Scegli automaticamente**. Per configurare le opzioni di aggiornamento avanzate, ad esempio la modalità di aggiornamento, l'accesso al server proxy, le connessioni LAN e la creazione di copie delle firme antivirali, fare clic sul pulsante **Configurazione...**.



3.3 Configurazione del server proxy

Nel caso in cui si utilizzi un server proxy per controllare le connessioni a Internet su un sistema che utilizza ESET File Security, deve essere specificato nella finestra Configurazione avanzata. Per accedere alla finestra di configurazione del server proxy, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Varie** > **Server proxy** nella struttura Configurazione avanzata. Selezionare l'opzione **Utilizza server proxy**, quindi compilare i campi **Server proxy** (indirizzo IP) e **Porta**. Se necessario, selezionare l'opzione **Il server proxy richiede l'autenticazione**, quindi immettere **Nome utente** e **Password**.



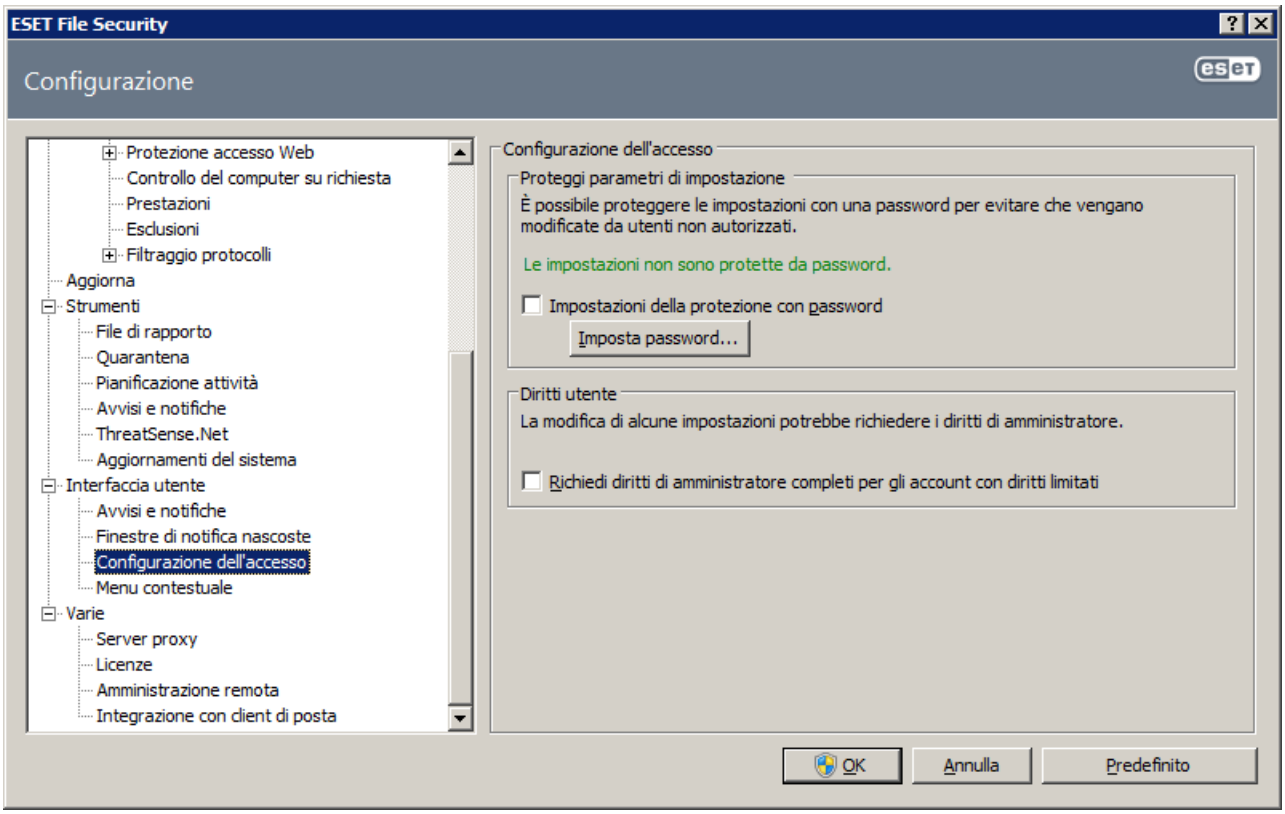
Se queste informazioni non sono disponibili, provare a rilevare automaticamente le impostazioni del server proxy facendo clic sul pulsante **Rileva server proxy**.

NOTA: le opzioni del server proxy potrebbero essere diverse in base ai diversi profili di aggiornamento. In questo caso, configurare i diversi profili di aggiornamento nella finestra Configurazione avanzata facendo clic su **Aggiorna** nella struttura Configurazione avanzata.

3.4 Protezione delle impostazioni

Le impostazioni di ESET File Security rivestono un ruolo fondamentale dal punto di vista dei criteri di protezione dell'azienda. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Per proteggere con password i parametri di configurazione, nel menu principale fare clic su **Configurazione** > **Immetti struttura di configurazione avanzata completa...** > **Interfaccia utente** > **Configurazione dell'accesso**, selezionare l'opzione **Proteggi impostazioni con password** e fare clic sul pulsante **Imposta password...**.

Immettere una nuova password nei campi **Nuova password** e **Conferma nuova password**, quindi fare clic su **OK**. La password verrà richiesta per apportare future modifiche a ESET File Security.



NOTA: fare clic qui per visualizzare come viene configurata tramite eShell.

4. Utilizzo di ESET File Security

4.1 ESET File Security - Protezione server

ESET File Security assicura la protezione del server con funzionalità essenziali quali: Antivirus e antispyware, scudo residente (Protezione in tempo reale), Protezione accesso Web e Protezione client di posta. Ulteriori informazioni su ciascun tipo di protezione sono disponibili nella sezione ESET File Security - Protezione computer. È inoltre disponibile la funzionalità Esclusioni automatiche che identifica le applicazioni server e i file del sistema operativo server critici e li aggiunge automaticamente all'elenco di Esclusioni. Questa funzionalità riduce al minimo il rischio di potenziali conflitti e migliora le prestazioni generali del server quando è in esecuzione il software antivirus.

4.1.1 Esclusioni automatiche

Gli sviluppatori delle applicazioni server e dei sistemi operativi consigliano di escludere i gruppi di file e cartelle di lavoro critici dai controlli antivirus per la maggior parte dei loro prodotti. I controlli antivirus possono esercitare un'influenza negativa sulle prestazioni di un server, creando conflitti e impedendo persino l'esecuzione di alcune applicazioni sul server. Le esclusioni aiutano a ridurre al minimo il rischio di potenziali conflitti e a migliorare le prestazioni generali del server quando è in esecuzione il software antivirus.

ESET File Security identifica le applicazioni server e i file del sistema operativo server critici e li aggiunge automaticamente all'elenco di Esclusioni. Una volta aggiunti all'elenco, è possibile attivare (per impostazione predefinita) il processo/applicazione server selezionando l'apposita casella o disattivarli deselezionandola, con il seguente risultato:

1) Se l'esclusione di un'applicazione/sistema operativo rimane attivata, uno qualsiasi dei file e cartelle critici verrà aggiunto all'elenco di file esclusi dal controllo (**Configurazione avanzata** > **Protezione computer** > **Antivirus e antispyware** > **Esclusioni**). A ogni riavvio del server, il sistema esegue un controllo automatico delle esclusioni e ripristina eventuali esclusioni che potrebbero essere state eliminate dall'elenco. Questa è l'impostazione consigliata se si desidera essere certi che siano sempre applicate le Esclusioni automatiche consigliate.
2) Se l'utente disattiva l'esclusione di un'applicazione/sistema operativo, i rispettivi file e cartelle critici rimangono nell'elenco di file esclusi dal controllo (**Configurazione avanzata** > **Protezione computer** > **Antivirus e antispyware** > **Esclusioni**). Tuttavia, non verranno controllati e rinnovati automaticamente sull'elenco **Esclusioni** a ogni riavvio del server (vedere precedente punto 1). Questa impostazione è consigliata agli utenti avanzati che desiderano rimuovere o modificare alcune delle esclusioni standard. Se si desidera che le esclusioni siano rimosse dall'elenco senza riavviare il server, sarà necessario rimuoverle manualmente dall'elenco (**Configurazione avanzata** > **Protezione computer** > **Antivirus e antispyware** > **Esclusioni)**.

Qualsiasi esclusione definita dall'utente manualmente in **Configurazione avanzata** > **Protezione computer** > **Antivirus e antispyware** > **Esclusioni** non sarà influenzata dalla impostazioni descritte in precedenza.

Le Esclusioni automatiche di applicazioni/sistemi operativi server vengono selezionate in base alle raccomandazioni Microsoft. Per informazioni dettagliate, vedere i seguenti collegamenti:

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

4.2 ESET File Security - Protezione computer

ESET File Security dispone di tutti gli strumenti necessari per garantire la protezione del server come un computer. Offre una protezione efficace al server con i seguenti tipi di protezione: Antivirus e antispyware, scudo residente (Protezione in tempo reale), Protezione accesso Web e Protezione client di posta.

4.2.1 Protezione antivirus e antispyware

La protezione antivirus difende il sistema da attacchi dannosi controllando file, messaggi e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla: prima bloccandola e poi pulendola, eliminandola o mettendola in quarantena.

4.2.1.1 Protezione file system in tempo reale

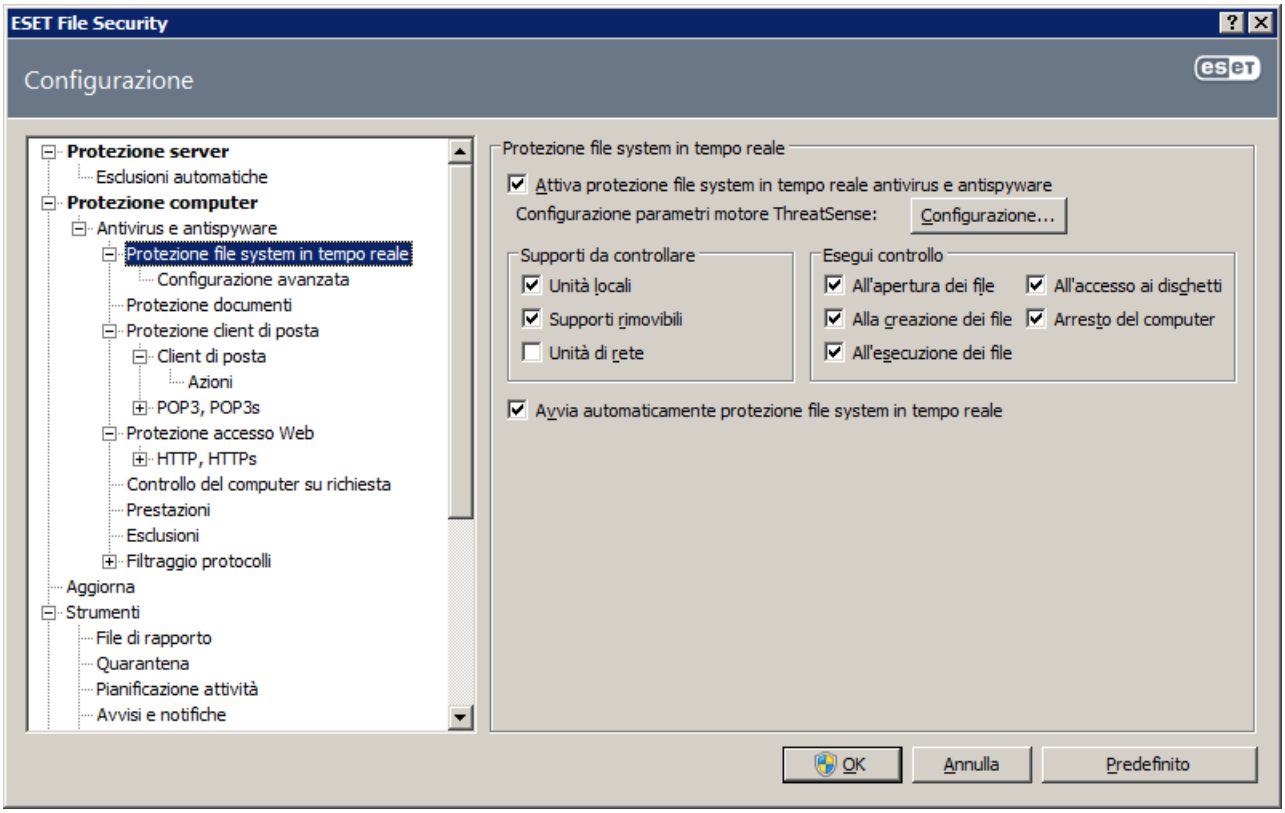
La funzione di Protezione file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus nel sistema. Tutti i file vengono sottoposti a controllo alla ricerca di codice dannoso nel momento in cui vengono aperti, creati o eseguiti sul computer. La funzione Protezione file system in tempo reale viene avviata all'avvio del sistema.

4.2.1.1.1 Configurazione del controllo

La funzione Protezione file system in tempo reale controlla tutti i tipi di supporto quando si verificano determinati eventi. Grazie ai metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione Configurazione parametri motore ThreatSense), la protezione file system in tempo reale potrebbe variare rispetto ai file appena creati o a quelli esistenti. Nel caso di file appena creati è possibile applicare un livello di controllo maggiore.

Per ridurre al minimo l'impatto sul sistema quando si utilizza la protezione in tempo reale, i file già sottoposti a controllo non vengono controllati ripetutamente, a meno che non siano stati modificati. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali. Questo comportamento viene configurato mediante la funzione Ottimizzazione Smart. Quando questa funzione è disattivata, tutti i file vengono controllati a ogni accesso. Per modificare questa opzione, aprire la finestra Configurazione avanzata e fare clic su **Antivirus e antispyware** > **Protezione file system in tempo reale** nella struttura Configurazione avanzata. Selezionare quindi il pulsante **Configurazione...** accanto a **Configurazione parametri motore ThreatSense**, fare clic su **Altro** e selezionare o deselezionare l'opzione **Attiva ottimizzazione Smart**.

In base alle impostazioni predefinite, la protezione in tempo reale viene avviata automaticamente all'avvio del sistema operativo e fornisce un controllo ininterrotto. In casi particolari (ad esempio, in caso di conflitto con un altro scanner in tempo reale), la protezione in tempo reale può essere arrestata disattivando l'opzione **Avvia automaticamente la protezione file system in tempo reale**.



4.2.1.1.1.1 Supporti da controllare

Per impostazione predefinita, vengono controllati tutti i tipi di supporto alla ricerca di eventuali minacce.

Unità locali - Consente di controllare tutte le unità disco rigido del sistema

Supporti rimovibili - Dischetti, supporti di archiviazione USB e così via.

Unità di rete - Consente di eseguire il controllo di tutte le unità mappate

Si consiglia di mantenere le impostazioni predefinite e di modificarle solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

4.2.1.1.1.2 Controllo al verificarsi di un evento

Per impostazione predefinita, tutti i file sono sottoposti a controllo all'apertura, durante la creazione o l'esecuzione. È consigliabile mantenere le impostazioni predefinite che offrono il massimo livello di protezione in tempo reale per il computer.

L'opzione **All'accesso ai dischetti** consente di controllare il settore di avvio dei dischetti quando si accede all'unità. L'opzione **Arresto del computer** consente il controllo dei settori di avvio del disco rigido durante l'arresto del computer. Sebbene i virus del settore di avvio siano oggi piuttosto rari, è consigliabile lasciare attivate queste opzioni poiché esiste ancora la possibilità di infezione di un virus del settore di avvio da fonti alternative.

4.2.1.1.1.3 Opzioni avanzate di controllo

In **Protezione computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale** > **Configurazione avanzata** sono disponibili opzioni di configurazione più dettagliate.

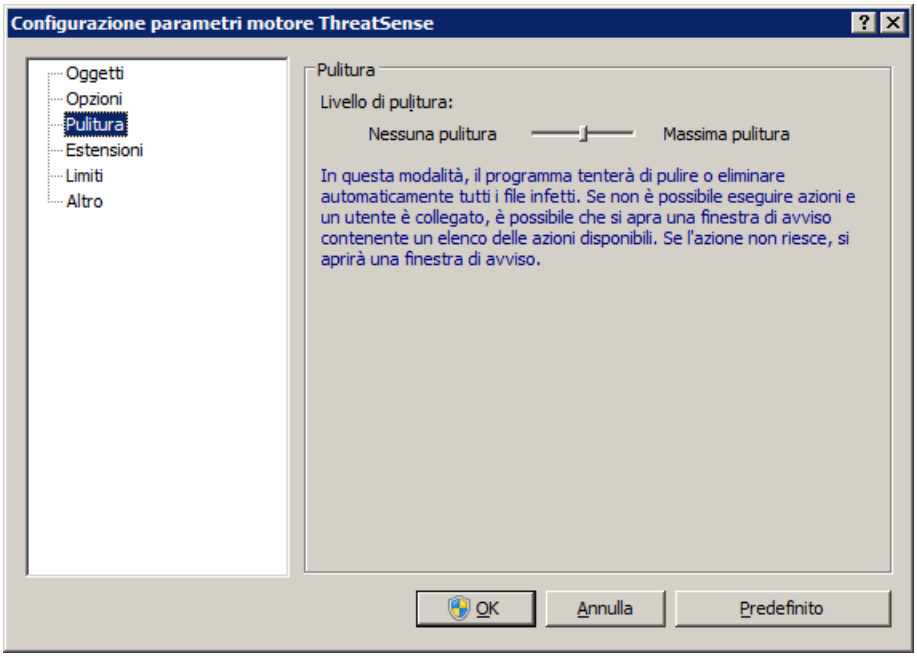
Parametri ThreatSense aggiuntivi per i file appena creati e modificati - I file appena creati o modificati hanno maggiore possibilità di essere infettati rispetto a quelli esistenti. Per questo motivo il programma controlla tali file con parametri aggiuntivi. Oltre ai comuni metodi di controllo basati sulle firme, viene utilizzata la funzione di euristica avanzata che consente un notevole miglioramento delle percentuali di rilevamento. Oltre che sui file appena creati, il controllo viene eseguito anche sui file autoestraenti (SFX) e sugli eseguibili compressi, ovvero file eseguibili compressi a livello interno. Per impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e controllati indipendentemente dalla loro dimensione effettiva. Per modificare le impostazioni di controllo dell'archivio, deselezionare l'opzione Impostazioni predefinite controllo degli archivi.

Parametri ThreatSense.Net aggiuntivi per i file eseguiti - Per impostazione predefinita, quando i file vengono eseguiti non viene usata l'euristica avanzata. In alcuni casi potrebbe tuttavia essere utile attivare questa opzione (selezionando l'opzione **Euristica avanzata all'esecuzione dei file**). È possibile che l'euristica avanzata rallenti l'esecuzione di alcuni programmi a causa dell'aumento dei requisiti di sistema.

4.2.1.1.2 Livelli di pulitura

La protezione in tempo reale prevede tre livelli di pulitura. Per selezionare un livello di pulitura, fare clic sul pulsante **Configurazione...** nella sezione **Protezione file system in tempo reale** e fare clic sulla sottostruttura **Pulitura**.

- Il primo livello, **Nessuna pulitura**, visualizza una finestra di avviso contenente le opzioni a disposizione per ciascuna infiltrazione trovata. È necessario scegliere un'azione da eseguire per ciascuna singola infiltrazione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.
- Il livello predefinito sceglie ed esegue automaticamente un'azione predefinita (a seconda del tipo di infiltrazione). Un messaggio nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Le azioni automatiche non vengono eseguite se l'infiltrazione si trova all'interno di un archivio, il quale contiene anche i file puliti, o quando agli oggetti infetti non è associata un'azione predefinita.
- Il terzo livello, **Massima pulitura**, è quello più "aggressivo" in quanto tutti gli oggetti infetti vengono puliti. Poiché questo livello potrebbe eventualmente comportare la perdita di file validi, si consiglia di utilizzarlo solo in situazioni specifiche.


Configurazione parametri motore ThreatSense
Oggetti
Opzioni
Pulitura
Estensioni
Limiti
Altro
Pulitura
Livello di pulitura:
Nessuna pulitura
Massima pulitura
In questa modalità, il programma tenterà di pulire o eliminare automaticamente tutti i file infetti. Se non è possibile eseguire azioni e un utente è collegato, è possibile che si apra una finestra di avviso contenente un elenco delle azioni disponibili. Se l'azione non riesce, si aprirà una finestra di avviso.
OK
Annulla
Predefinito

4.2.1.1.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Prestare quindi la massima attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici, ad esempio se si verifica un conflitto con una determinata applicazione o con lo scanner in tempo reale di un altro programma antivirus.

Dopo l'installazione di ESET File Security, tutte le impostazioni sono ottimizzate al fine di offrire il massimo livello di protezione del sistema agli utenti. Per ripristinare le impostazioni predefinite, fare clic sul pulsante **Impostazioni predefinite** posizionato in basso a destra della finestra **Protezione file system in tempo reale** (**Configurazione avanzata** > **Antivirus e antispyware** > **Protezione file system in tempo reale**).

4.2.1.1.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Questo file di test è un file innocuo, speciale e rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus. Può essere scaricato all'indirizzo http://www.eicar.org/download/eicar.com

NOTA: prima di eseguire un controllo della protezione in tempo reale, è necessario disattivare il firewall. Se il firewall è attivato, rileverà e impedirà di scaricare i file di test.

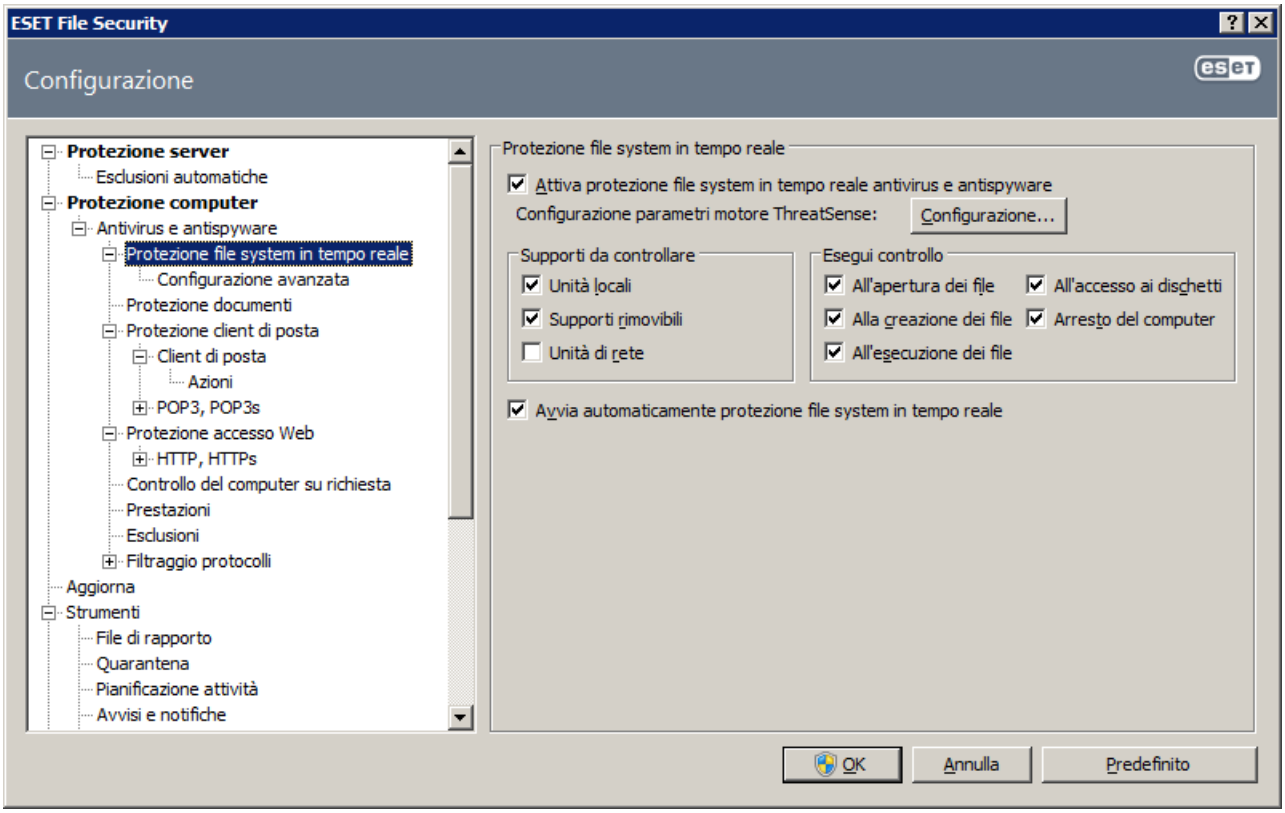
4.2.1.1.5 Cosa fare se la protezione in tempo reale non funziona

Nel capitolo successivo verranno illustrate situazioni problematiche che potrebbero verificarsi quando si utilizza la protezione in tempo reale e verranno descritte le relative modalità di risoluzione.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, accedere a **Configurazione** > **Antivirus e antispyware** e fare clic su **Attiva nella sezione Protezione file system in tempo reale** della finestra del programma principale.

Se la protezione in tempo reale non viene avviata all'avvio del sistema, è probabile che l'opzione **Avvia automaticamente la protezione file system in tempo reale** non sia attivata. Per attivare l'opzione, accedere a Configurazione avanzata (F5) e fare clic su **Protezione file system in tempo reale** nella struttura Configurazione avanzata. Nella sezione **Configurazione avanzata** nella parte inferiore della finestra, verificare che la casella di controllo **Avvia automaticamente la protezione file system in tempo reale** sia selezionata.



La protezione in tempo reale non rileva né pulisce le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene avviata all'avvio del sistema (e l'opzione **Avvia automaticamente la protezione file system in tempo reale** è attivata), è probabile che entri in conflitto con altri programmi. In questo caso, consultare gli specialisti del Supporto tecnico di ESET.

4.2.1.2 Protezione client di posta

La Protezione client di posta garantisce il controllo delle comunicazioni via e-mail ricevute mediante il protocollo POP3. Utilizzando il programma plugin per Microsoft Outlook, ESET File Security controlla tutte le comunicazioni dal client di posta (POP3, MAPI, IMAP, HTTP).

Durante la verifica dei messaggi in arrivo, vengono utilizzati tutti i metodi di controllo avanzato forniti dal motore di controllo ThreatSense. Ciò significa che il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il database delle firme antivirali. Il controllo delle comunicazioni mediante il protocollo POP3 non dipende dal client di posta in uso.

4.2.1.2.1 Controllo POP3

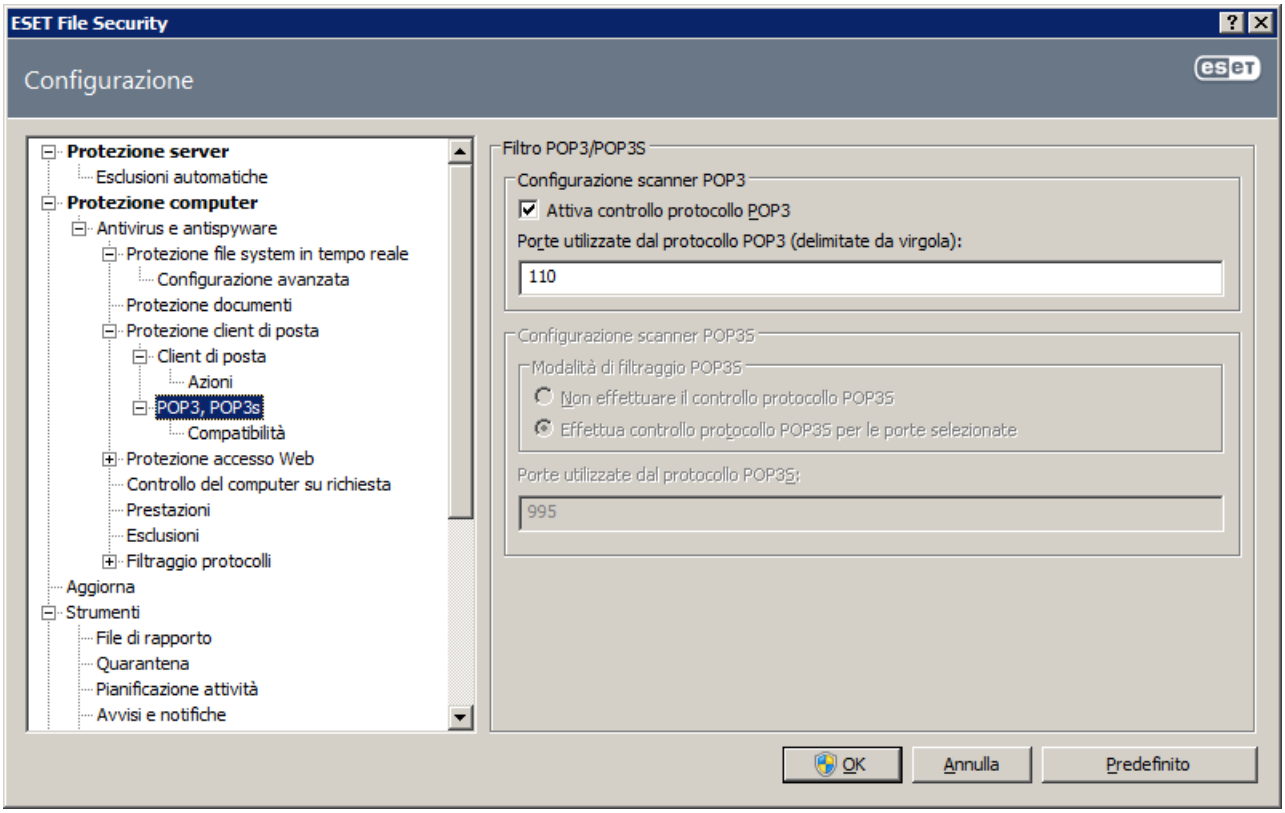
Il protocollo POP3 è quello più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client di posta. ESET File Security offre la protezione per questo protocollo, indipendentemente dal client di posta in uso.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Affinché il modulo funzioni correttamente, verificare che sia attivato: il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono sottoposte a controllo tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

Le comunicazioni crittografate non sono controllate.

Per poter utilizzare il filtraggio POP3/POP3S, è prima necessario attivare il Filtraggio protocolli. Se le opzioni POP3/POP3S non sono selezionabili, accedere a **Protezione computer** > **Antivirus e antispyware** > **Filtraggio protocolli** dalla struttura Configurazione avanzata e selezionare l'opzione **Attiva filtro del contenuto del protocollo di**

applicazioni. Per ulteriori informazioni sul filtro e sulla configurazione, consultare la sezione Filtraggio protocolli.



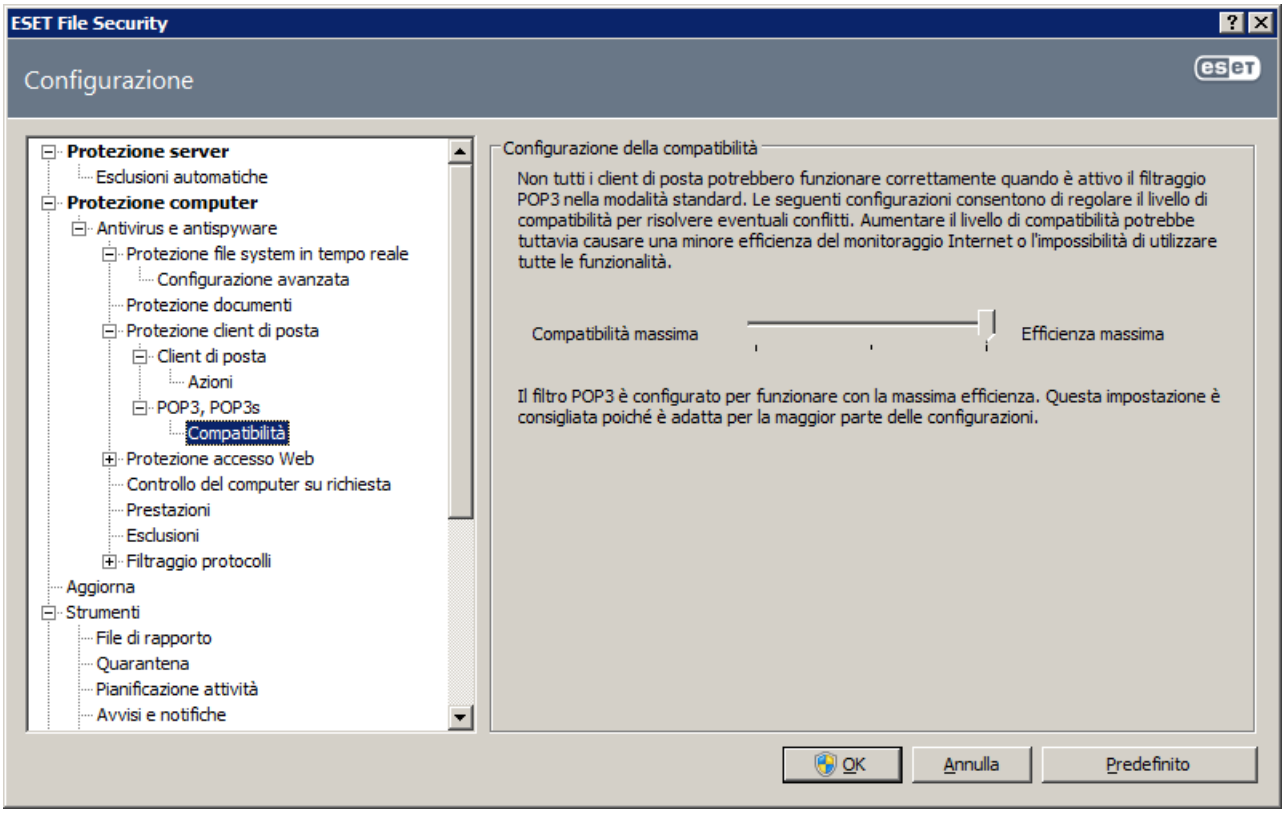
4.2.1.2.1.1 Compatibilità

Alcuni programma di posta possono riscontrare problemi con il filtraggio POP3, ad esempio se si ricevono messaggi con una connessione Internet lenta, potrebbero verificarsi timeout a seguito del controllo eseguito. In questo caso, provare e modificare le modalità di esecuzione del controllo. La riduzione del livello di controllo può migliorare la velocità della procedura di pulitura. Per regolare il livello di controllo del filtraggio POP3, dalla struttura Configurazione avanzata accedere a **Antivirus e antispyware** > **Protezione e-mail** > **POP3, POP3s** > **Compatibilità** .

Se l'opzione **Efficienza massima** è attivata, le infiltrazioni vengono eliminate dai messaggi infetti e le informazioni sull'infiltrazione vengono inserite davanti all'oggetto del messaggio e-mail originale (è necessario che le opzioni **Elimina** o **Pulisci** siano attivate o che sia attivato il livello di pulitura **massima** o **predefinita**).

L'opzione **Compatibilità media** consente di modificare la modalità di ricezione dei messaggi. I messaggi vengono inviati gradualmente al client di posta. Dopo che il messaggio è stato trasferito, viene sottoposto al controllo alla ricerca di infiltrazioni. Con questo livello di controllo, il rischio di infezione è maggiore. Il livello di pulitura e la gestione dei messaggi contrassegnati, ovvero gi avvisi di notifica allegati alla riga dell'oggetto e al testo dei messaggi e-mail, sono identici all'impostazione Massima efficienza.

Il livello **Compatibilità massima** consente di visualizzare una finestra di avviso per segnalare all'utente la ricezione di un messaggio infetto. Nessuna informazione sui file infetti viene aggiunta alla riga dell'oggetto o al testo dei messaggi consegnati e le infiltrazioni non vengono eliminate automaticamente ma è necessario che l'utente le cancelli dal client di posta.

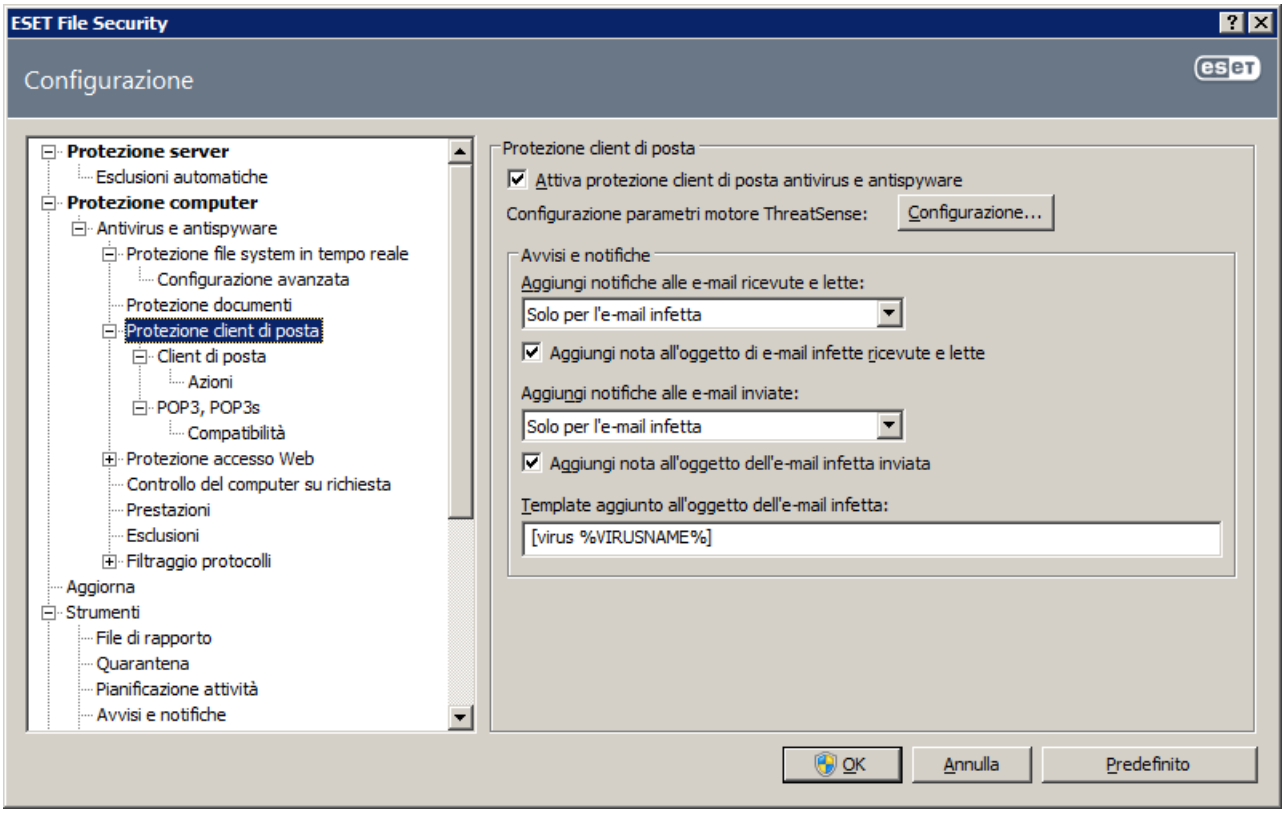

ESET File Security
Configurazione
Protezione server
Esclusioni automatiche
Protezione computer
Antivirus e antispyware
Protezione file system in tempo reale
Configurazione avanzata
Protezione documenti
Protezione client di posta
Client di posta
Azioni
POP3, POP3s
Compatibilità
Protezione accesso Web
Controllo del computer su richiesta
Prestazioni
Esclusioni
Filtraggio protocolli
Aggiorna
Strumenti
File di rapporto
Quarantena
Pianificazione attività
Avvisi e notifiche
Configurazione della compatibilità
Non tutti i client di posta potrebbero funzionare correttamente quando è attivo il filtraggio POP3 nella modalità standard. Le seguenti configurazioni consentono di regolare il livello di compatibilità per risolvere eventuali conflitti. Aumentare il livello di compatibilità potrebbe tuttavia causare una minore efficienza del monitoraggio Internet o l'impossibilità di utilizzare tutte le funzionalità.
Compatibilità massima
Efficienza massima
Il filtro POP3 è configurato per funzionare con la massima efficienza. Questa impostazione è consigliata poiché è adatta per la maggior parte delle configurazioni.
OK
Annulla
Predefinito

4.2.1.2.2 Integrazione con client di posta

L'integrazione di ESET File Security con i client di posta aumenta il livello di protezione attiva contro codici dannosi nei messaggi e-mail. Se il client di posta in uso è supportato, tale integrazione può essere attivata in ESET File Security. Se l'integrazione viene attivata, la barra degli strumenti di ESET File Security viene inserita direttamente nel client di posta, consentendo una protezione e-mail più efficace. Le impostazioni di integrazione sono disponibili nella sezione **Configurazione** > **Immetti struttura di configurazione avanzata completa...** > **Varie** > **Integrazione con client di posta**. L'integrazione con il client di posta consente di attivare l'integrazione con i client di posta supportati. I client di posta attualmente supportati includono Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

Selezionare l'opzione **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento del sistema durante l'utilizzo del client di posta. Una situazione simile può verificarsi durante il download dei messaggi e-mail da Kerio Outlook Connector Store.

Per attivare la protezione e-mail fare clic su **Configurazione** > **Immetti struttura di configurazione avanzata completa...** > **Antivirus e antispyware** > **Protezione client di posta** e selezionare l'opzione **Attiva protezione client di posta antivirus e antispyware**.



4.2.1.2.2.1 Aggiunta di notifiche al testo dei messaggi e-mail

Ciascun messaggio e-mail controllato da ESET File Security può essere contrassegnato aggiungendo una notifica all'oggetto o al testo del messaggio. Questa funzione aumenta il livello di credibilità del destinatario e se viene rilevata un'infiltrazione, fornisce informazioni utili sul livello di minaccia di un determinato messaggio o mittente.

Le opzioni per questa funzionalità sono disponibili nella sezione **Configurazione avanzata** > **Antivirus e antispyware** > **Protezione client di posta**. È possibile selezionare **Aggiungi notifiche alle e-mail ricevute e lette**, nonché **Aggiungi notifica alle e-mail inviate**. È inoltre possibile scegliere se aggiungere le notifiche a tutti i messaggi e-mail sottoposti al controllo, solo a quelli infetti o se non aggiungerle.

ESET File Security consente anche di aggiungere messaggi all'oggetto originale dei messaggi infetti. Per attivare l'aggiunta all'oggetto, selezionare entrambe le opzioni **Aggiungi nota all'oggetto di e-mail infette ricevute e lette** e **Aggiungi nota all'oggetto dell'e-mail infetta inviata**.

Il contenuto delle notifiche può essere modificato nel campo **Template aggiunto all'oggetto dell'e-mail infetta**. Le modifiche indicate sopra possono facilitare l'automazione del processo di filtraggio dei messaggi e-mail infetti in quanto consentono all'utente di filtrare i messaggi e-mail con oggetto specifico, se supportato dal client di posta, in una cartella separata.

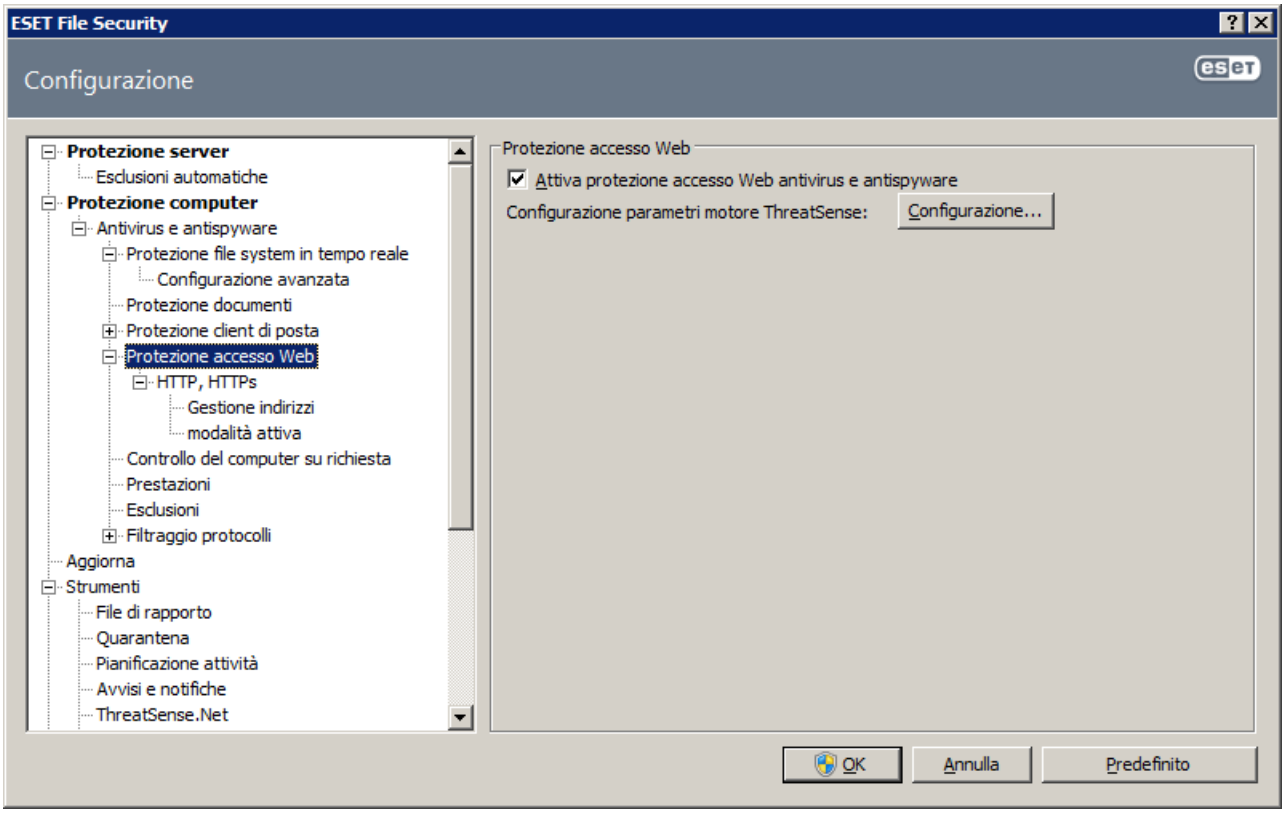
4.2.1.2.3 Eliminazione delle infiltrazioni

In caso di ricezione di messaggi e-mail infetti, verrà visualizzata una finestra di avviso contenente il nome del mittente, il messaggio e-mail e il nome dell'infiltrazione. Nella parte inferiore della finestra, sono disponibili le opzioni **Pulisci**, **Elimina** o **Nessuna azione** per l'oggetto rilevato. Nella maggior parte dei casi è consigliabile selezionare **Pulisci** o **Elimina**. In alcuni casi, se si desidera comunque ricevere il file infetto, selezionare **Nessuna azione**.

Se è attivata l'opzione **Massima pulitura**, verrà visualizzata una finestra di informazioni, senza nessuna opzione disponibile per gli oggetti infetti.

4.2.1.3 Protezione accesso Web

La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. Per tale motivo, è essenziale gestire in modo accurato la Protezione accesso Web. Si consiglia di attivare l'opzione **Attiva protezione accesso Web antivirus e antispyware**. Questa opzione è disponibile in **Configurazione avanzata** (F5) > **Antivirus e antispyware** > **Protezione accesso Web**.

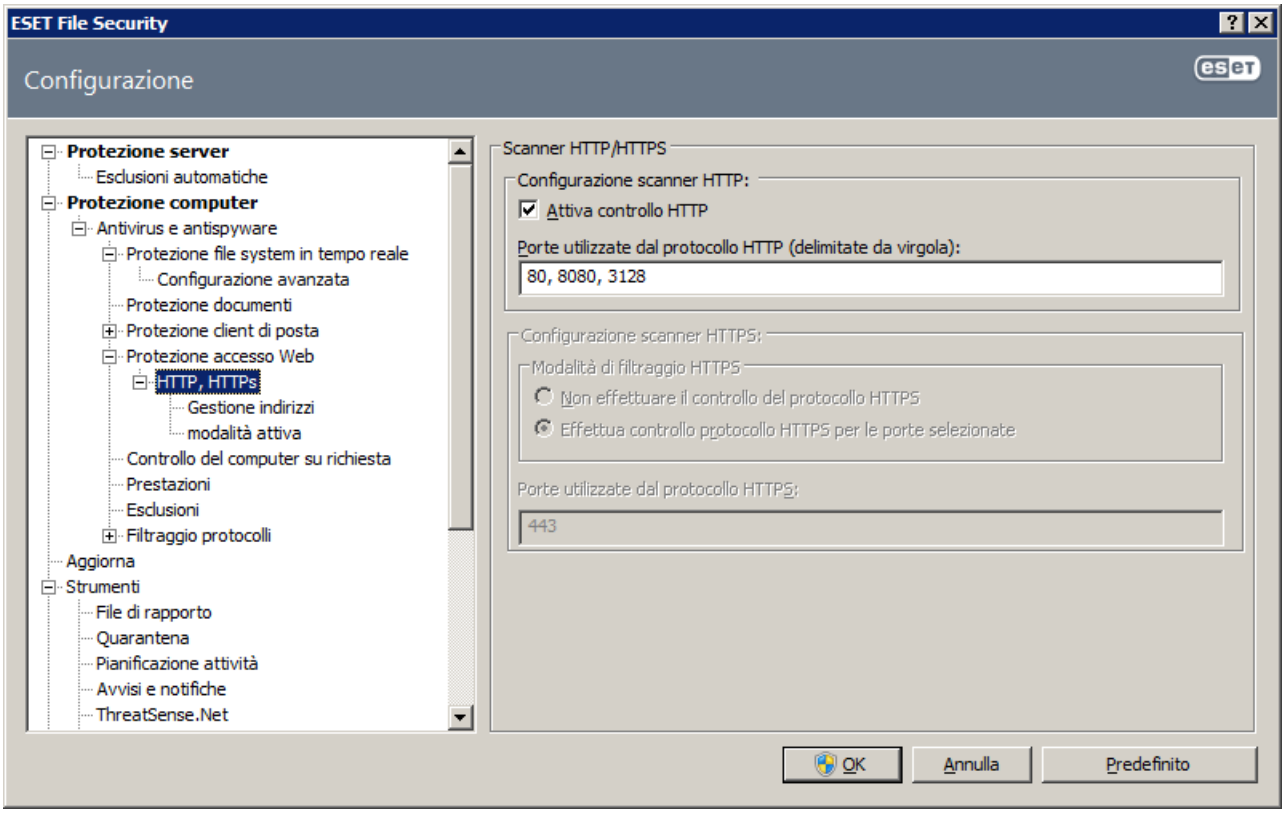


4.2.1.3.1 HTTP, HTTPS

La Protezione accesso Web monitora la comunicazione tra i browser Internet e i server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata). Per impostazione predefinita, ESET File Security è configurato in modo da utilizzare gli standard della maggior parte dei browser Internet. Le opzioni di impostazione dello scanner HTTP possono tuttavia essere modificate in **Configurazione avanzata** (F5) > **Antivirus e antispyware** > **Protezione accesso Web** > **HTTP, HTTPS**. Nella finestra principale del filtro HTTP è possibile selezionare o deselezionare l'opzione **Attiva controllo HTTP**. È inoltre possibile definire i numeri delle porte utilizzate per la comunicazione HTTP. L'impostazione predefinita per i numeri delle porte è 80, 8080 e 3128. Il controllo HTTPS può essere impostato con le seguenti modalità:

Non effettuare il controllo del protocollo HTTPS - La comunicazione crittografata non verrà controllata

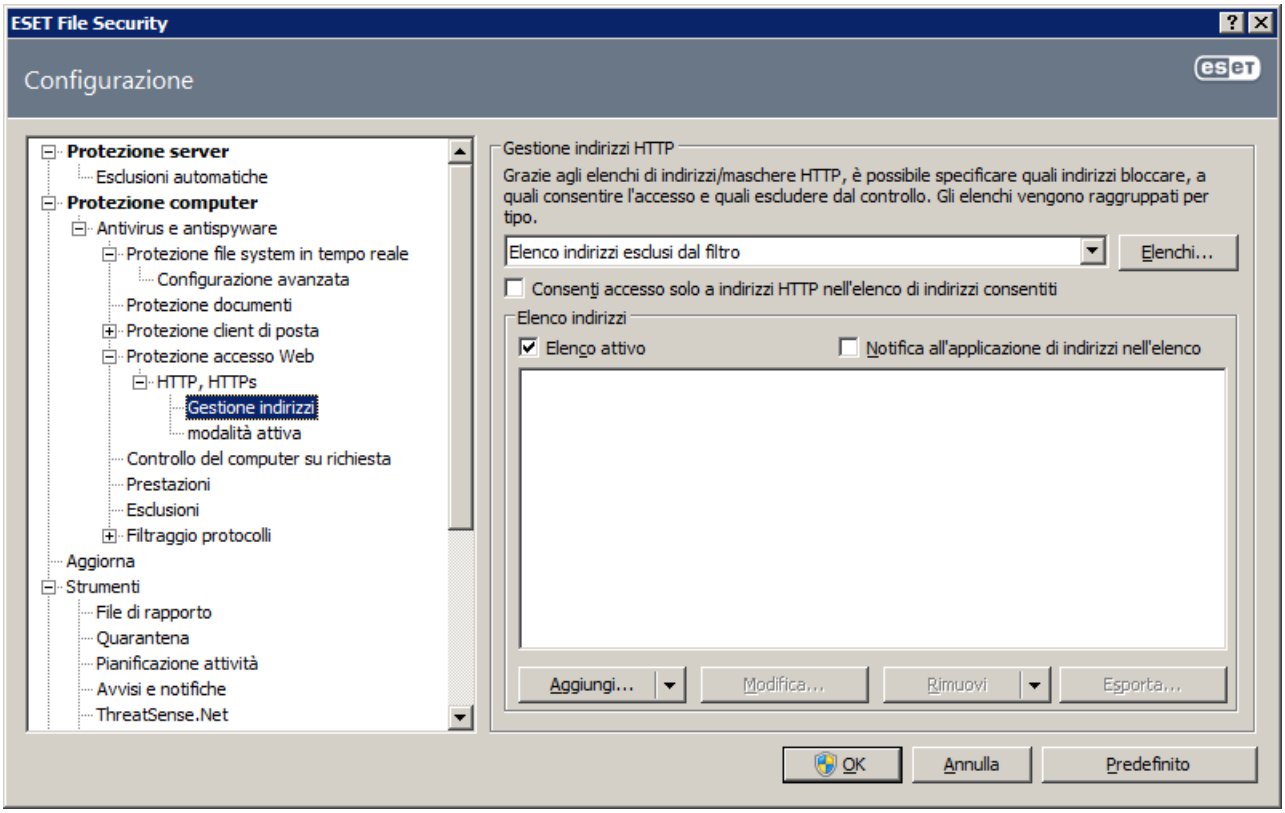
Effettua controllo protocollo HTTPS per le porte selezionate - Il controllo HTTPS viene utilizzato solo per le porte definite in **Porte utilizzate dal protocollo HTTPS**.



4.2.1.3.1.1 Gestione indirizzo

Questa sezione consente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo. I pulsanti **Aggiungi...**, **Modifica...**, **Rimuovi** ed **Esporta...** vengono utilizzati per gestire l'elenco degli indirizzi. Non sarà possibile accedere ai siti Web presenti nell'elenco degli indirizzi bloccati. Durante l'accesso, i siti Web presenti nell'elenco degli indirizzi esclusi non vengono sottoposti al controllo per rilevare il codice dannoso. Se è attivata l'opzione **Consenti accesso solo agli indirizzi HTTP dell'elenco indirizzi consentiti**, sarà possibile accedere solo agli indirizzi presenti nell'elenco degli indirizzi consentiti, mentre gli altri indirizzi HTTP verranno bloccati.

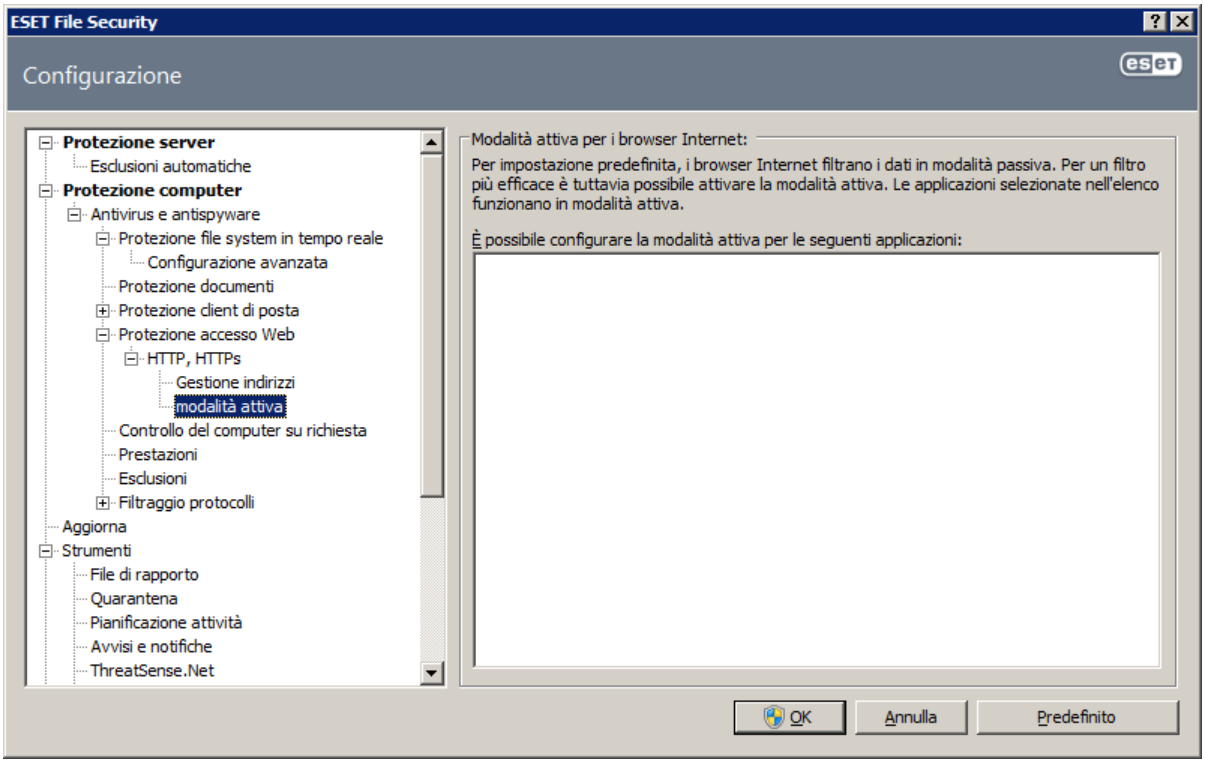
In tutti gli elenchi è possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri, mentre il punto interrogativo sostituisce qualsiasi simbolo. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, poiché l'elenco deve contenere solo indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente. Per attivare l'elenco, selezionare l'opzione **Elenco attivo**. Se si desidera ricevere una notifica quando viene immesso un indirizzo dall'elenco corrente, selezionare l'opzione **Notifica all'applicazione di indirizzi nell'elenco**.



4.2.1.3.1.2 Modalità attiva

L'elenco delle applicazioni contrassegnate come browser Web è accessibile direttamente dal sottomenu **Browser Web** della sottostruttura **HTTP, HTTPS**. Questa sezione contiene anche il sottomenu **Modalità attiva** che definisce la modalità di controllo per i browser Internet.

La **Modalità attiva** è utile poiché esamina i dati trasferiti nel suo insieme. Se non è attivata, la comunicazione delle applicazioni viene monitorata gradualmente in batch. Questo può ridurre l'efficacia del processo di verifica dei dati, ma fornisce anche una maggiore compatibilità per le applicazioni elencate. Se non si verificano problemi durante il relativo utilizzo, è consigliabile attivare la modalità attiva di controllo selezionando la casella di controllo accanto all'applicazione desiderata.



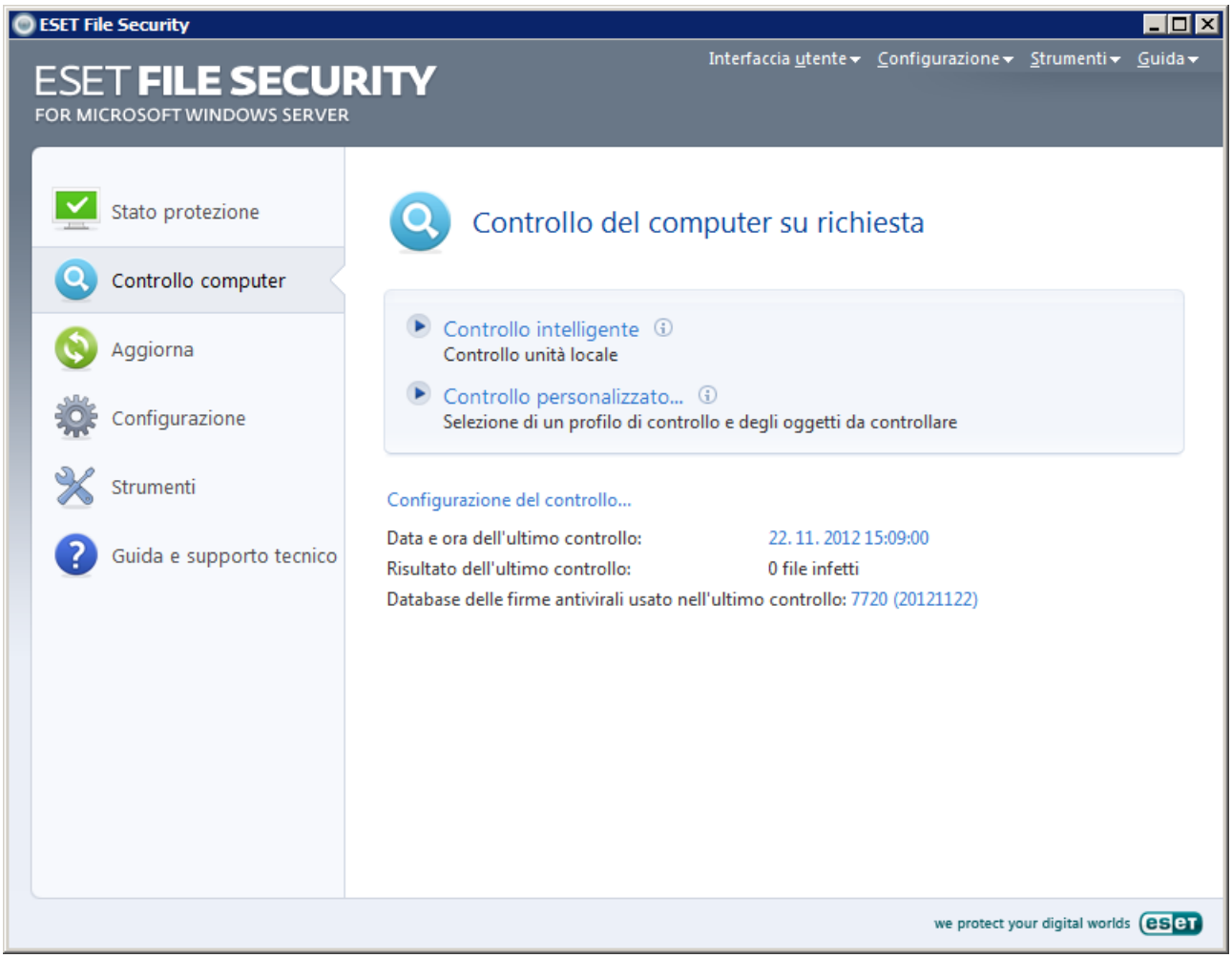
4.2.1.4 Controllo del computer su richiesta

Se si sospetta che il computer sia infettato, ovvero se si comporta in maniera anomala, eseguire un Controllo del computer su richiesta per esaminare il computer alla ricerca di infiltrazioni. Dal punto di vista della protezione, è essenziale che i controlli del computer non vengano eseguiti solo quando si sospetta un'infezione, ma periodicamente, nell'ambito delle normali misure di protezione. Il controllo periodico consente infatti di rilevare le infiltrazioni che non sono state rilevate dallo scanner in tempo reale durante il salvataggio sul disco. Ciò può verificarsi se lo scanner in tempo reale è stato disattivato nel momento in cui si è manifestata l'infezione o le il database delle firme antivirali non è aggiornato.

È consigliabile eseguire un Controllo del computer su richiesta almeno una volta al mese. Il controllo può essere configurato come attività pianificata in **Strumenti** > **Pianificazione attività**.

4.2.1.4.1 Tipo di controllo

Sono disponibili due tipologie di Controllo computer su richiesta. **Controllo intelligente** consente di eseguire rapidamente il controllo del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato...** consente di selezionare uno dei profili di controllo predefiniti, nonché di scegliere oggetti da controllare specifici.



4.2.1.4.1.1 Controllo intelligente

La funzione Controllo intelligente consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. I principali vantaggi consistono nel semplice utilizzo, senza necessità di dover eseguire una configurazione dettagliata del controllo. Il Controllo intelligente consente di effettuare un controllo di tutti i file presenti nelle unità locali, nonché una pulitura o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulitura viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di pulitura, consultare la sezione Pulitura.

4.2.1.4.1.2 Controllo personalizzato

Il controllo personalizzato è una soluzione ottimale se si desidera specificare parametri di controllo quali oggetti da controllare e metodi di controllo. Il vantaggio del Controllo personalizzato è la possibilità di configurare i parametri in dettaglio. È possibile salvare le configurazioni come profili di controllo definiti dagli utenti che risultano particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri.

Per scegliere gli oggetti da controllare, selezionare **Controllo computer** > **Controllo personalizzato**, quindi selezionare un'opzione dal menu a discesa **Oggetti da controllare** oppure selezionare oggetti specifici dalla struttura ad albero. Un oggetto da controllare può anche essere specificato in maniera più precisa immettendo il percorso della cartella o dei file che si desidera includere. Se si desidera controllare solo il sistema senza ulteriori azioni di pulitura, selezionare l'opzione **Controllo senza rimozione**. È inoltre possibile scegliere tra tre livelli di pulitura selezionando **Configurazione...** > **Pulitura**.

4.2.1.4.2 Oggetti da controllare

Il menu a discesa Oggetti da controllare consente di selezionare file, cartelle e dispositivi (dischi) da controllare alla ricerca di virus.

Attraverso le impostazioni di profilo - Consente di selezionare le destinazioni nel profilo di controllo selezionato

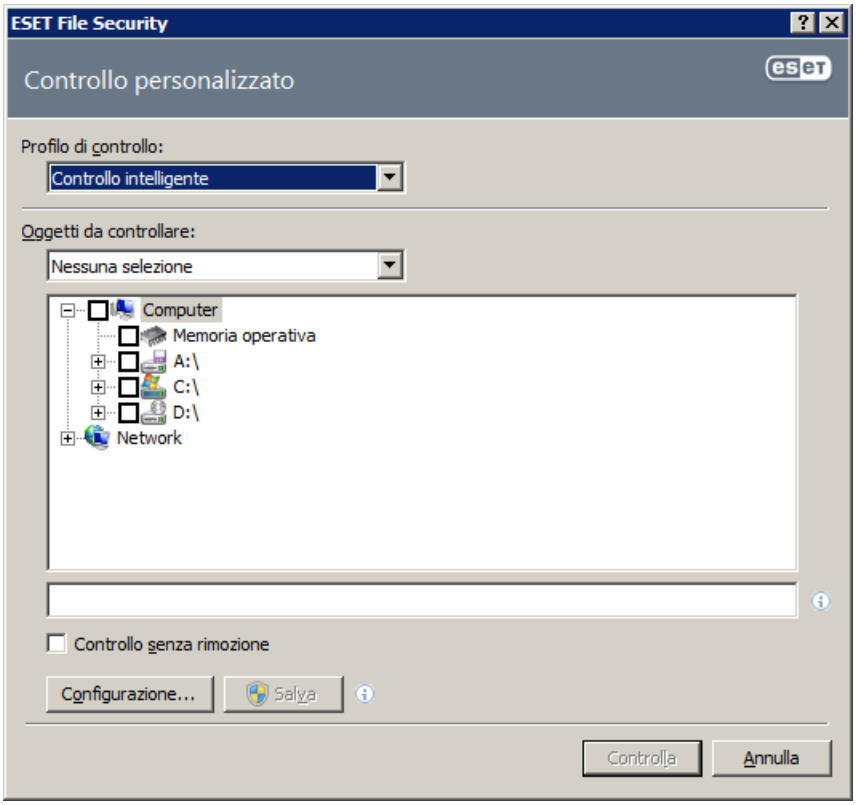
Supporti rimovibili - Consente di selezionare dischetti, supporti di archiviazione USB, CD/DVD

Unità locali - Consente di selezionare tutte le unità disco rigido del sistema

Unità di rete - Consente di selezionare tutte le unità mappate

Nessuna selezione - Consente di annullare tutte le selezioni

Un oggetto da controllare può anche essere specificato immettendo il percorso della cartella o dei file che si desidera includere nel controllo. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i dispositivi disponibili nel computer.

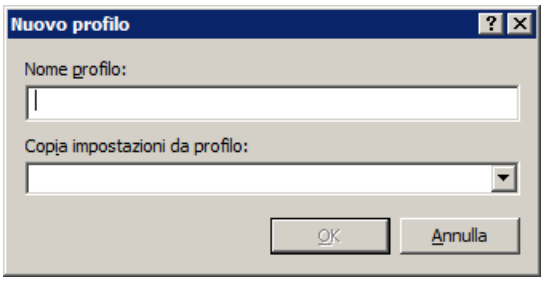


4.2.1.4.3 Profili di controllo

È possibile salvare i parametri di controllo preferiti per i controlli futuri. È consigliabile creare un profilo di controllo differente (con diversi oggetti da controllare, metodi di controllo e altri parametri) per ciascun controllo utilizzato abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Controllo computer su richiesta** > **Profili...** Nella finestra **Profili di configurazione** è disponibile un menu a discesa contenente i profili di controllo esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza nella creazione di un profilo di controllo adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione del controllo.

ESEMPIO: si supponga di voler creare il proprio profilo di controllo e che la configurazione del Controllo intelligente sia appropriata solo in parte, in quanto non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose, bensì si intende applicare l'opzione **Massima pulitura**. Nella finestra **Profili di configurazione**, fare clic sul pulsante **Aggiungi...**. Immettere il nome del nuovo profilo nel campo **Nome profilo**, quindi selezionare **Controllo intelligente** dal menu a discesa **Copia impostazioni dal profilo** . Regolare quindi gli altri parametri in base ai requisiti specifici.



4.2.1.4.4 Riga di comando

Il modulo antivirus di ESET File Security può essere avviato dalla riga di comando, manualmente con il comando "ecls" oppure con un file batch ("bat").

È possibile utilizzare i parametri e le opzioni riportati di seguito quando viene eseguito un controllo su richiesta dalla riga di comando:

Opzioni generali:

- help	mostra Guida ed esci
- version	mostra informazioni sulla versione ed esci
- base-dir = FOLDER	carica moduli da CARTELLA
- quar-dir = FOLDER	CARTELLA di quarantena
- aind	mostra indicatore di attività

Destinazioni:

- files	esegui controllo dei file (impostazione predefinita)
- no-files	non eseguire controllo dei file
- boots	esegui controllo dei settori di avvio (impostazione predefinita)
- no-boots	non eseguire controllo dei settori di avvio
- arch	esegui controllo degli archivi (impostazione predefinita)
- no-arch	non eseguire controllo degli archivi
- max-archive-level = LEVEL	LIVELLO massimo di nidificazione degli archivi
- scan-timeout = LIMIT	esegui controllo degli archivi per LIMITE secondi al massimo. Se il tempo di esecuzione del controllo supera tale limite, il controllo dell'archivio viene interrotto e il controllo proseguirà sul prossimo file.
- max-arch-size=SIZE	esegui controllo solo dei primi byte della DIMENSIONE negli archivi (impostazione predefinita 0 = illimitata)
- mail	esegui controllo dei file di e-mail
- no-mail	non eseguire controllo dei file di e-mail
- sfx	esegui controllo degli archivi autoestraenti
- no-sfx	non eseguire controllo degli archivi autoestraenti
- rtp	esegui controllo degli eseguibili compressi
- no-rtp	non eseguire controllo degli eseguibili compressi
- exclude = FOLDER	escludi CARTELLA dal controllo
- subdir	esegui controllo delle sottocartelle (impostazione predefinita)
- no-subdir	non eseguire controllo delle sottocartelle
- max-subdir-level = LEVEL	LIVELLO massimo di nidificazione delle sottocartelle (impostazione predefinita 0 = illimitato)
- symlink	segui i collegamenti simbolici (impostazione predefinita)
- no-symlink	ignora collegamenti simbolici

- ext-remove = EXTENSIONS	
- ext-exclude = EXTENSIONS	escludi dal controllo le ESTENSIONI delimitate da due punti

Metodi:

- adware	esegui il controllo di Adware/Spyware/Riskware
- no-adware	non eseguire controllo di Adware/Spyware/Riskware
- unsafe	esegui controllo delle applicazioni potenzialmente pericolose
- no-unsafe	non eseguire il controllo delle applicazioni potenzialmente pericolose
- unwanted	esegui controllo delle applicazioni potenzialmente indesiderate
- no-unwanted	non eseguire il controllo delle applicazioni potenzialmente indesiderate
- pattern	utilizza firme
- no-pattern	non utilizzare le firme digitali
- heur	attiva l'euristica
- no-heur	disattiva l'euristica
- adv-heur	attiva l'euristica avanzata
- no-adv-heur	disattiva l'euristica avanzata

Pulitura:

- action = ACTION	esegui AZIONE sugli oggetti infettati. Azioni disponibili: nessuna, pulitura, chiedi
- quarantine	copia i file infettati in Quarantena (integra AZIONE)
- no-quarantine	non copiare file infettati in Quarantena

Rapporti:

- log-file=FILE	registra output nel FILE
- log-rewrite	sovrascrivi il file di output (impostazione predefinita: aggiungi)
- log-all	registra anche file puliti
- no-log-all	non registrare file puliti (impostazione predefinita)

Possibili codici di uscita del controllo:

0	- nessuna minaccia rilevata
1	- minaccia rilevata ma non pulita
10	- rimasti alcuni file infetti
101	- errore archivio
102	- errore di accesso
103	- errore interno

NOTA: i codici di uscita superiori a 100 indicano che non è stato eseguito il controllo del file, il quale potrebbe

quindi essere infetto.

4.2.1.5 Prestazioni

In questa sezione è possibile configurare il numero dei motori di controllo ThreatSense che verranno utilizzati per il controllo dei virus. Maggiore è il numero dei motori di controllo ThreatSense sulle macchie multiprocessore, maggiore è la velocità di controllo. Il valore accettabile è compreso tra 1 e 20.

Se non sono presenti altre restrizioni, è consigliabile aumentare il numero dei motori di controllo ThreatSense nella finestra Impostazioni avanzate (F5) in **Protezione computer** > **Antivirus e antispyware** > **Prestazioni**, in base alle seguente formula: *numero di motori di controllo ThreatSense = (numero di CPU fisiche x 2) + 1*. Di seguito viene riportato un esempio:

Si supponga di avere un server con 4 CPU fisiche. In base alla precedente formula, per ottenere prestazioni ottimali si dovrebbe disporre di 9 motori di controllo.

NOTA: le modifiche apportate in questa sezione avranno effetto solo al successivo riavvio.

4.2.1.6 Filtraggio protocolli

La protezione antivirus per i protocolli di applicazione POP3 e HTTP viene fornita tramite il motore di controllo ThreatSense, che integra perfettamente tutte le tecniche di controllo avanzate dei malware. Il controllo funziona automaticamente, indipendentemente dal browser o dal client di posta in uso. Per il filtraggio protocolli sono disponibili le seguenti opzioni (se è selezionata l'opzione **Attiva filtro del contenuto del protocollo di applicazioni**):

Porte HTTP e POP3 - Limita il controllo delle comunicazioni alle porte HTTP e POP3 note.

Applicazioni contrassegnate come browser Web e client di posta - Attivare questa opzione per filtrare solo le comunicazioni delle applicazioni contrassegnate come browser (**Protezione accesso Web** > **HTTP, HTTPS** > **Browser Web**) e client di posta (**Protezione client di posta** > **POP3, POP3s** > **Client di posta**).

Porte e applicazioni contrassegnate come browser Web o client di posta - Viene eseguito il controllo alla ricerca di malware sulle porte e sui browser.

NOTA: in Windows Vista Service Pack 1 e Windows Server 2008 viene utilizzato un nuovo metodo di filtraggio delle comunicazioni. La sezione Filtraggio protocolli non è pertanto disponibile.

4.2.1.6.1 SSL

ESET File Security consente di verificare i protocolli incapsulati nel protocollo SSL. È possibile utilizzare varie modalità di controllo per le comunicazioni protette mediante il protocollo SSL utilizzando certificati attendibili, certificati sconosciuti o certificati che sono esclusi dalla verifica delle comunicazioni protette mediante il protocollo SSL.

Effettua sempre controllo del protocollo SSL - Selezionare questa opzione per verificare tutte le comunicazioni protette mediante il protocollo SSL ad eccezione delle comunicazioni protette mediante i certificati esclusi dalla verifica. Se viene stabilita una nuova comunicazione usando un certificato firmato sconosciuto, all'utente non verrà inviata alcuna notifica e la comunicazione verrà filtrata in modo automatico. Quando si accede a un server con un certificato non attendibile contrassegnato dall'utente come attendibile (ovvero aggiunto all'elenco dei certificati attendibili), la comunicazione con il server è consentita e il contenuto del canale di comunicazione viene filtrato.

Chiedi conferma per siti non visitati (è possibile configurare esclusioni) - Se si accede a un nuovo sito protetto SSL (con un certificato sconosciuto), verrà visualizzata una finestra di dialogo in cui è possibile scegliere l'azione da eseguire. Questa modalità consente di creare un elenco di certificati SSL che verranno esclusi dal controllo.

Non controllare il protocollo SSL - Se viene selezionata questa opzione, il programma non eseguirà il controllo delle comunicazioni su SSL.

Se il certificato non può essere verificato utilizzando l'archivio Autorità di certificazione radice attendibili (**Filtraggio protocolli** > **SSL** > **Certificati**):

Chiedi conferma della validità dei certificati - Chiede all'utente di scegliere l'azione da eseguire.

Blocca comunicazioni che utilizzano il certificato - Termina la connessione al sito che utilizza il certificato.

Se è il certificato non è valido o è danneggiato (**Filtraggio protocolli** > **SSL** > **Certificati**):

Chiedi conferma della validità dei certificati - Chiede all'utente di scegliere l'azione da eseguire.

Blocca comunicazioni che utilizzano il certificato - Termina la connessione al sito che utilizza il certificato.

4.2.1.6.1.1 Certificati attendibili

In aggiunta all'archivio Autorità di certificazione radice attendibili integrato dove ESET File Security archivia i certificati attendibili, è possibile creare un elenco personalizzato di certificati attendibili che possono essere visualizzati in **Configurazione avanzata** (F5) > **Filtraggio protocolli** > **SSL** > **Certificati** > **Certificati attendibili**.

4.2.1.6.1.2 Certificati esclusi

La sezione Certificati esclusi contiene i certificati ritenuti sicuri. Il contenuto delle comunicazioni crittografate che utilizzano i certificati nell'elenco non verrà verificato alla ricerca di minacce. È consigliabile escludere solo i certificati Web che sono garantiti come sicuri. In questo caso, non è necessario verificare la comunicazione che utilizza tali certificati.

4.2.1.7 Configurazione parametri motore ThreatSense

ThreatSense è una tecnologia costituita da numerosi metodi complessi di rilevamento delle minacce. Questa tecnologia è proattiva, ovvero fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Utilizza una combinazione di diversi metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per potenziare in modo significativo la protezione del sistema. Il motore di controllo è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di configurazione della tecnologia ThreatSense consentono di specificare vari parametri di controllo:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulitura e così via.

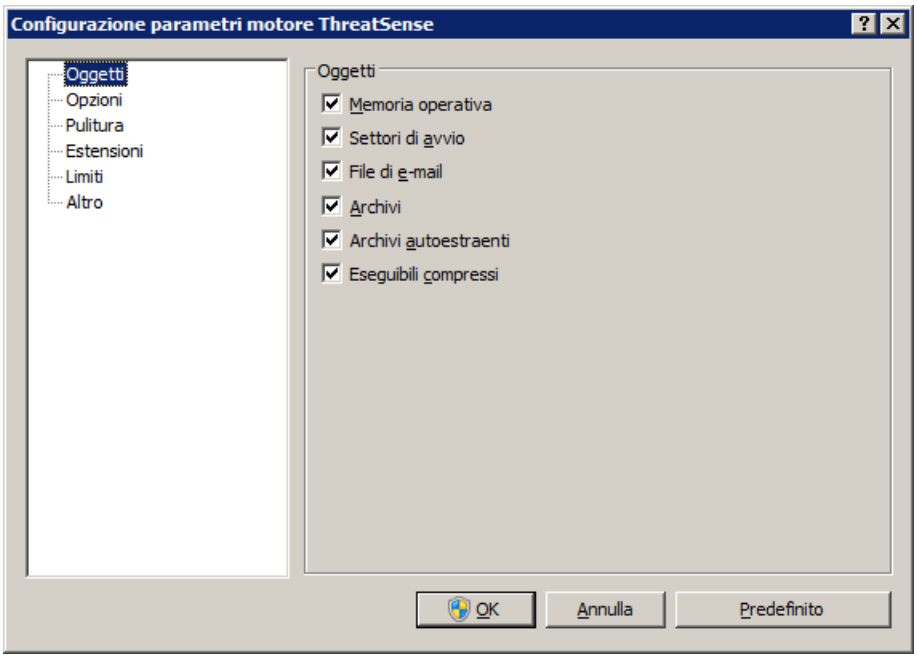
Per aprire la finestra di impostazione, fare clic sul pulsante **Configurazione...** presente in qualsiasi finestra di impostazione del modulo che utilizza la tecnologia ThreatSense (vedere di seguito). Scenari di protezione diversi possono richiedere configurazioni diverse. In considerazione di questo, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- Protezione file system in tempo reale
- Controllo del file di avvio del sistema
- Protezione e-mail
- Protezione accesso Web
- Controllo del computer su richiesta

I parametri ThreatSense sono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica dei parametri per il controllo degli eseguibili compressi o per consentire il controllo dell'euristica avanzata nel modulo di protezione del file system in tempo reale potrebbe causare un rallentamento del sistema (in genere solo i file appena creati sono sottoposti a controllo con questi metodi). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, ad eccezione di Controllo computer su richiesta.

4.2.1.7.1 Configurazione degli oggetti

Nella sezione **Oggetti** è possibile definire i componenti e file del computer che saranno sottoposti a controllo per la ricerca di infiltrazioni.



Memoria operativa - Consente di eseguire il controllo per la ricerca di minacce che attaccano la memoria operativa del sistema.

Settori di avvio - Consente di controllare i settori di avvio alla ricerca di virus nel record di avvio principale.

File - Consente di controllare tutti i tipi di file comuni (programmi, immagini, file audio e video, file di database e così via).

File di e-mail - Consente di controllare file speciali dove sono contenuti i messaggi e-mail.

Archivi - Consente di controllare i file compressi negli archivi (RAR, ZIP, ARJ, TAR e così via).

Archivi autoestraenti - Consente di controllare i file che sono contenuti negli file degli archivi autoestraenti ma presentati generalmente con un'estensione file EXE.

Eseguibili compressi - Gli eseguibili compressi, a differenza dei tipi di archivi standard, vengono decompressi nella memoria, in aggiunta agli eseguibili statici standard (UPX, yoda, ASPack, FGS e così via).

NOTA: quando accanto a un parametro viene visualizzato un punto blu, significa che l'impostazione corrente per quel parametro è differente dall'impostazione di altri moduli che utilizzano ThreatSense. Poiché per ciascun modulo è possibile configurare in maniera differente lo stesso parametro, il punto blu serve semplicemente a ricordare che quello stesso parametro è configurato in maniera differente per altri moduli. Se non è presente un punto blu, significa che il parametro è configurato uguale per tutti i moduli.

4.2.1.7.2 Opzioni

La sezione **Opzioni** consente di selezionare i metodi utilizzati durante un controllo del sistema per il rilevamento di eventuali infiltrazioni. Sono disponibili le seguenti opzioni:

Firme - Le firme sono in grado di rilevare e identificare in maniera esatta e affidabile le infiltrazioni in base al rispettivo nome grazie alle firme antivirus.

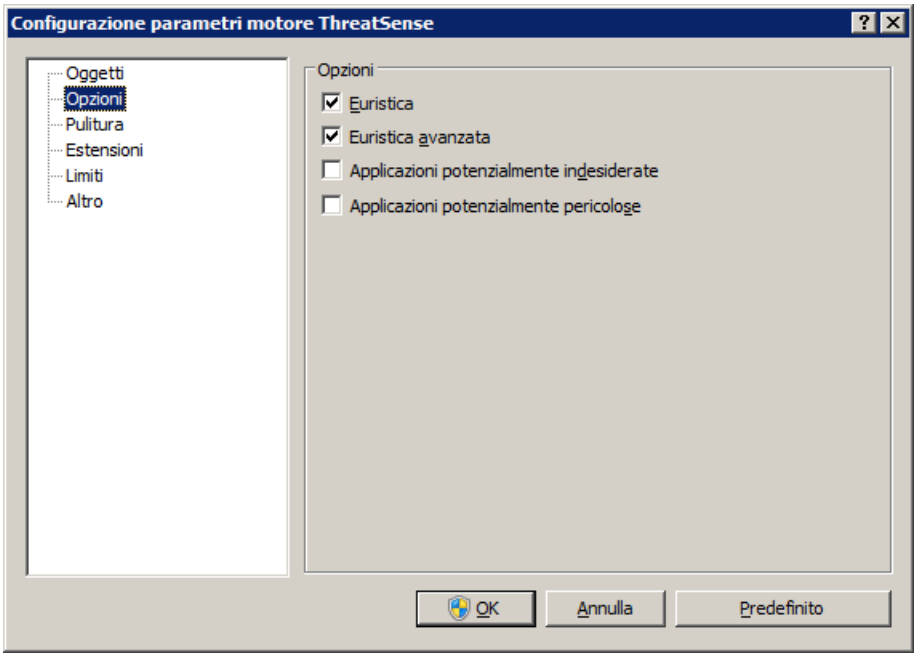
Euristica - L'euristica è un algoritmo che analizza l'attività (dannosa) dei programmi. Il vantaggio principale offerto dal rilevamento euristico consiste nella capacità di rilevare nuovo software dannoso precedentemente inesistente o non presente nell'elenco di virus noti, ovvero nel database delle firme antivirali.

Euristica avanzata - L'euristica avanzata si basa su un esclusivo algoritmo di euristica sviluppato da ESET, ottimizzato per il rilevamento dei worm e dei trojan horse e scritto in linguaggi di programmazione di alto livello. Grazie all'euristica avanzata, le capacità di rilevamento del programma sono significativamente più elevate.

Adware/Spyware/Riskware - Questa categoria include software che raccoglie varie informazioni sensibili sugli utenti senza il rispettivo consenso informato. In questa categoria rientra anche software che visualizza materiale pubblicitario.

Applicazioni potenzialmente indesiderate - Queste applicazioni non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative riguardano la visualizzazione di finestre popup indesiderata, l'attivazione e l'esecuzione di processi nascosti, il maggior utilizzo delle risorse di sistema, modifiche dei risultati di ricerca e applicazioni che comunicano con server remoti.

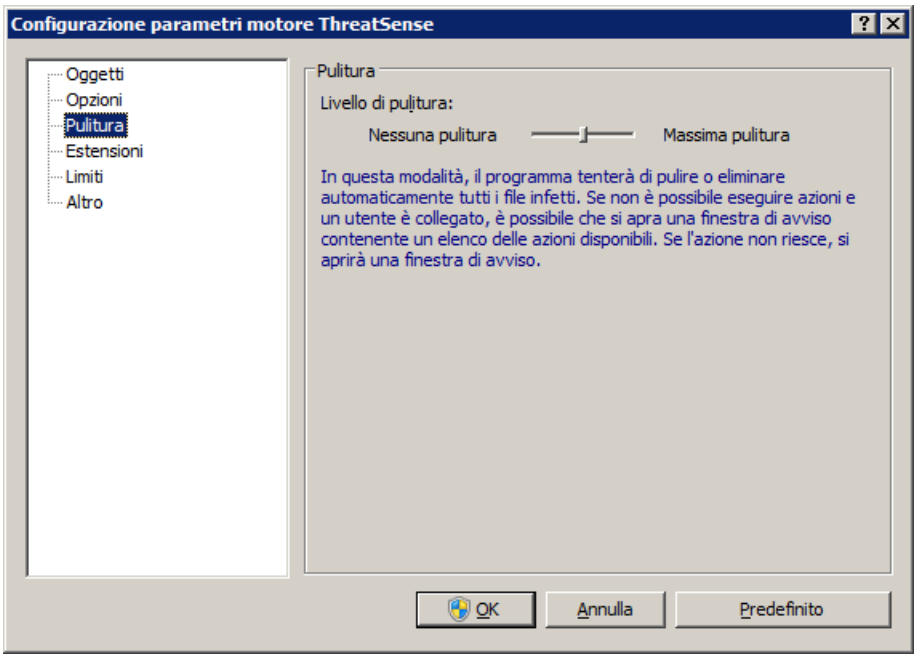
Applicazioni potenzialmente pericolose - È la classificazione utilizzata per il software legale e commerciale. Sono inclusi programmi quali gli strumenti di accesso remoto. Per tale motivo, questa opzione è disattivata per impostazione predefinita.



NOTA: quando accanto a un parametro viene visualizzato un punto blu, significa che l'impostazione corrente per quel parametro è differente dall'impostazione di altri moduli che utilizzano ThreatSense. Poiché per ciascun modulo è possibile configurare in maniera differente lo stesso parametro, il punto blu serve semplicemente a ricordare che quello stesso parametro è configurato in maniera differente per altri moduli. Se non è presente un punto blu, significa che il parametro è configurato uguale per tutti i moduli.

4.2.1.7.3 Pulitura

Le impostazioni di pulitura determinano il comportamento dello scanner durante la pulitura di file infetti. Sono disponibili 3 livelli di pulitura:


Configurazione parametri motore ThreatSense
Oggetti
Opzioni
Pulitura
Estensioni
Limiti
Altro
Pulitura
Livello di pulitura:
Nessuna pulitura
Massima pulitura
In questa modalità, il programma tenterà di pulire o eliminare automaticamente tutti i file infetti. Se non è possibile eseguire azioni e un utente è collegato, è possibile che si apra una finestra di avviso contenente un elenco delle azioni disponibili. Se l'azione non riesce, si aprirà una finestra di avviso.
OK
Annulla
Predefinito

Nessuna pulitura - I file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione.

Pulitura standard - Il programma tenterà di pulire o eliminare automaticamente un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre una scelta di azioni consigliate. La scelta di azioni consigliate verrà offerta anche nel caso in cui non sia stato possibile eseguire un'azione predefinita.

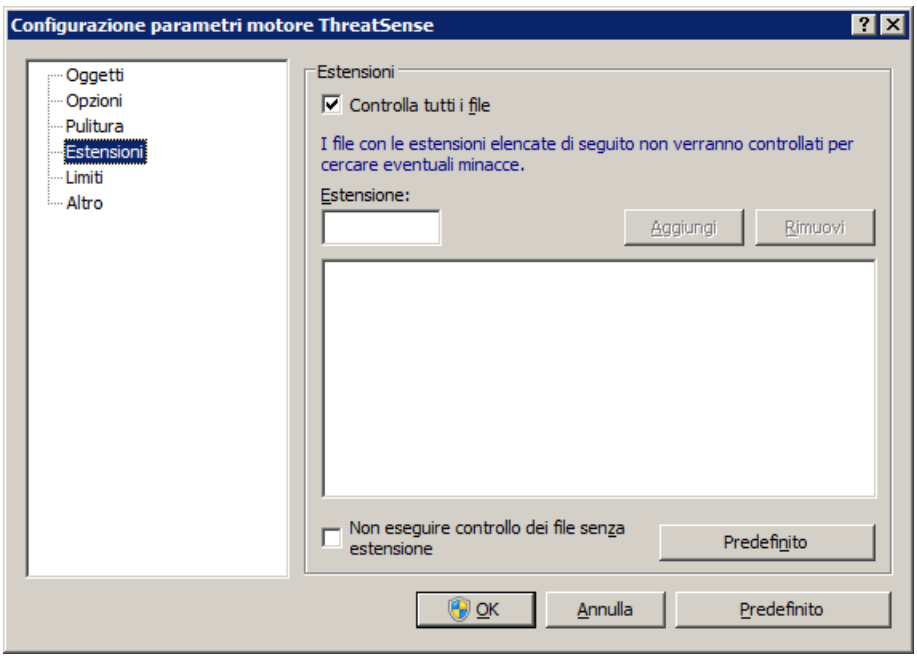
Massima pulitura - Il programma pulirà o eliminerà tutti i file infetti, compresi gli archivi. Le uniche eccezioni sono costituite dai file di sistema. Nel caso in cui non sia possibile pulirli, verrà visualizzata una finestra di avviso con la possibilità di scegliere un'azione da eseguire.

Attenzione: nella modalità di pulitura predefinita, l'intero file dell'archivio verrà eliminato solo se tutti i file all'interno di esso sono infetti. Se nell'archivio sono presenti anche file legittimi, non verrà eliminato. Se nella modalità Massima pulitura viene rilevato un file dell'archivio infetto, l'intero archivio verrà eliminato, anche nel caso in cui siano presenti file puliti.

NOTA: quando accanto a un parametro viene visualizzato un punto blu, significa che l'impostazione corrente per quel parametro è differente dall'impostazione di altri moduli che utilizzano ThreatSense. Poiché per ciascun modulo è possibile configurare in maniera differente lo stesso parametro, il punto blu serve semplicemente a ricordare che quello stesso parametro è configurato in maniera differente per altri moduli. Se non è presente un punto blu, significa che il parametro è configurato uguale per tutti i moduli.

4.2.1.7.4 Estensioni

Un'estensione è una parte del nome di un file delimitata da un punto. L'estensione definisce il tipo e il contenuto del file. Questa sezione delle impostazioni dei parametri ThreatSense consente di definire i tipi di file da sottoporre a controllo.



Per impostazione predefinita, tutti i file vengono sottoposti a controllo indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dal controllo. Se l'opzione **Controlla tutti i file** è deselezionata, l'elenco viene modificato per mostrare le estensioni di tutti i file sottoposti attualmente a controllo. I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire il controllo di estensioni specifiche.

Per attivare il controllo dei file senza estensione, selezionare l'opzione **Controlla file senza estensione**.

L'esclusione di file dal controllo è utile nel caso in cui il controllo di determinati tipi di file impedisse il corretto funzionamento di un programma che utilizzi le estensioni. Ad esempio, potrebbe essere consigliabile escludere le estensioni EDB, EML e TMP durante l'utilizzo dei server Microsoft Exchange.

NOTA: quando accanto a un parametro viene visualizzato un punto blu, significa che l'impostazione corrente per quel parametro è differente dall'impostazione di altri moduli che utilizzano ThreatSense. Poiché per ciascun modulo è possibile configurare in maniera differente lo stesso parametro, il punto blu serve semplicemente a ricordare che quello stesso parametro è configurato in maniera differente per altri moduli. Se non è presente un punto blu, significa che il parametro è configurato uguale per tutti i moduli.

4.2.1.7.5 Limiti

La sezione Limiti consente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire il controllo:

Dimensione massima oggetto: - Determina la dimensione massima degli oggetti da sottoporre al controllo. Il modulo antivirus eseguirà unicamente il controllo degli oggetti di dimensioni inferiori a quelle specificate. Si consiglia di non modificare i valori predefiniti in quanto, di norma, non sussiste alcun motivo per farlo. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dal controllo.

Durata massima controllo dell'oggetto (sec.): - Consente di definire il valore massimo di tempo destinato al controllo di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà il controllo dell'oggetto una volta raggiunto tale valore, indipendentemente dal fatto che il controllo sia stato completato.

Livello di ricerca degli archivi: - Specifica il livello massimo di controllo degli archivi. Si consiglia di non modificare il valore predefinito di 10. In circostanze normali, non sussiste alcun motivo per farlo. Se il controllo viene terminato anticipatamente a causa del numero di archivi nidificati, l'archivio non verrà selezionato.

Dimensione massima file in archivio: - Questa opzione consente di specificare le dimensioni massime dei file

contenuti all'interno degli archivi, i quali, una volta estratti, saranno sottoposti al controllo. Se per tale motivo il controllo dell'archivio viene terminato anticipatamente, l'archivio non verrà selezionato.

NOTA: quando accanto a un parametro viene visualizzato un punto blu, significa che l'impostazione corrente per quel parametro è differente dall'impostazione di altri moduli che utilizzano ThreatSense. Poiché per ciascun modulo è possibile configurare in maniera differente lo stesso parametro, il punto blu serve semplicemente a ricordare che quello stesso parametro è configurato in maniera differente per altri moduli. Se non è presente un punto blu, significa che il parametro è configurato uguale per tutti i moduli.

4.2.1.7.6 Altro

Controllo alternate data streams - I flussi di dati alternativi utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle tecniche di controllo standard. Molte infiltrazioni cercano di non essere rilevate presentandosi come flussi di dati alternativi.

Esegui controlli in background con priorità bassa - Ogni sequenza di controllo utilizza una determinata quantità di risorse del sistema. Se si utilizzano programmi che necessitano di molte risorse di sistema, è possibile attivare il controllo in background con priorità bassa e risparmiare risorse per le applicazioni.

Registra tutti gli oggetti - Se questa opzione è selezionata, il file di rapporto riporta tutti i file sottoposti a controllo, anche quelli non infetti.

Attiva ottimizzazione Smart - Selezionare questa opzione in modo che i file che sono già stati sottoposti a controllo non vengano controllati ripetutamente, a meno che non siano stati modificati. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali.

Mantieni timestamp ultimo accesso - Selezionare questa opzione per mantenere la data e l'ora di accesso originali ai file su cui è stato eseguito il controllo anziché aggiornarli (ad esempio, per l'utilizzo di sistemi di backup dei dati).

Scorri rapporto - Questa opzione consente di abilitare/disabilitare lo scorrimento del rapporto. Se selezionata, è possibile scorrere le informazioni verso l'alto nella finestra di visualizzazione.

Visualizza notifica sul completamento del controllo in una finestra separata - Apre una finestra indipendente contenente informazioni sui risultati del controllo.

NOTA: quando accanto a un parametro viene visualizzato un punto blu, significa che l'impostazione corrente per quel parametro è differente dall'impostazione di altri moduli che utilizzano ThreatSense. Poiché per ciascun modulo è possibile configurare in maniera differente lo stesso parametro, il punto blu serve semplicemente a ricordare che quello stesso parametro è configurato in maniera differente per altri moduli. Se non è presente un punto blu, significa che il parametro è configurato uguale per tutti i moduli.

4.2.1.8 Rilevamento di un'infiltrazione

Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio pagine Web, cartelle condivise, messaggi e-mail o supporti rimovibili (USB, dischi esterni, CD, DVD, dischetti e così via).

Se il computer mostra segnali di infezione malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile attenersi alle seguenti istruzioni:

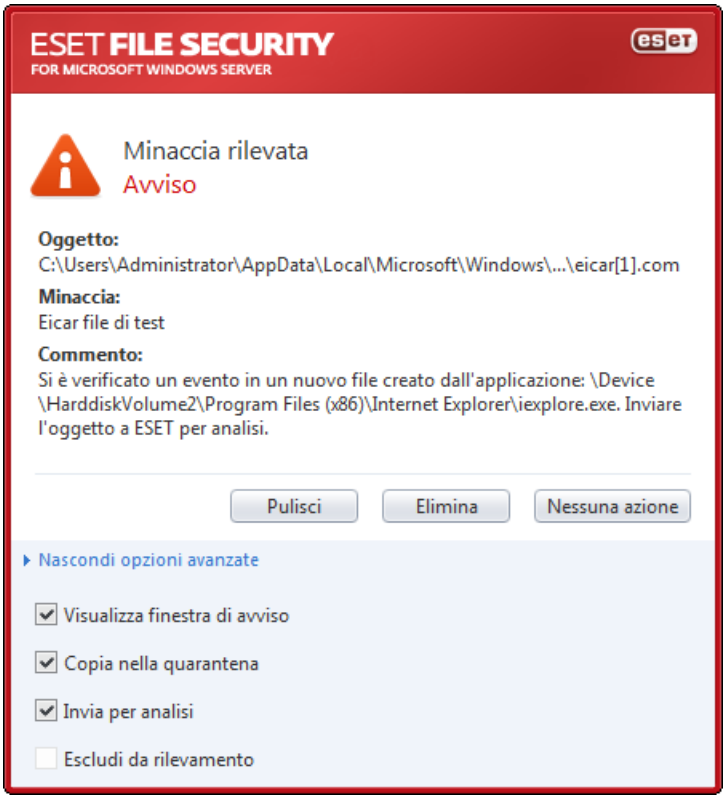
- Aprire ESET File Security e fare clic su Controllo computer
- Fare clic su **Controllo intelligente** (per ulteriori informazioni, consultare la sezione Controllo intelligente)
- Al termine del controllo, verificare nel registro il numero di file sottoposti a controllo, file infetti e file puliti.

Se si desidera effettuare il controllo solo di una parte del disco, scegliere **Controllo personalizzato** e selezionare gli oggetti da controllare alla ricerca di virus.

Per avere un'idea generale di come ESET File Security gestisce le infiltrazioni, si supponga che la Protezione file system in tempo reale, che utilizza il livello di pulitura predefinito, rilevi un'infiltrazione. Verrà eseguito il tentativo di pulire o eliminare il file. In assenza di azioni predefinite nel modulo di protezione in tempo reale, verrà chiesto all'utente di selezionare un'opzione in una finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, poiché con tale opzione si lasciano i file infetti inalterati. È opportuno selezionare questa opzione solo quando si è certi che il file non è pericoloso e che si tratta di un errore di rilevamento.

Pulitura ed eliminazione - Applicare la pulitura nel caso in cui un file sia stato attaccato da un virus che ha aggiunto un codice dannoso al file. In tal caso, tentare innanzitutto di pulire il file infetto per ripristinarne lo stato

originale. Nel caso in cui il file sia composto esclusivamente da codice dannoso, verrà eliminato.



Se un file infetto è "bloccato" o utilizzato da un processo del sistema, verrà eliminato solo dopo essere stato rilasciato (generalmente dopo il riavvio del sistema).

Eliminazione dei file negli archivi - Nella modalità di pulitura predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. È tuttavia consigliabile essere prudenti durante l'esecuzione di un controllo di massima pulitura: con tale modalità di pulitura l'archivio verrà eliminato nel caso in cui contenga almeno un file infetto, indipendentemente dallo stato degli altri file dell'archivio.

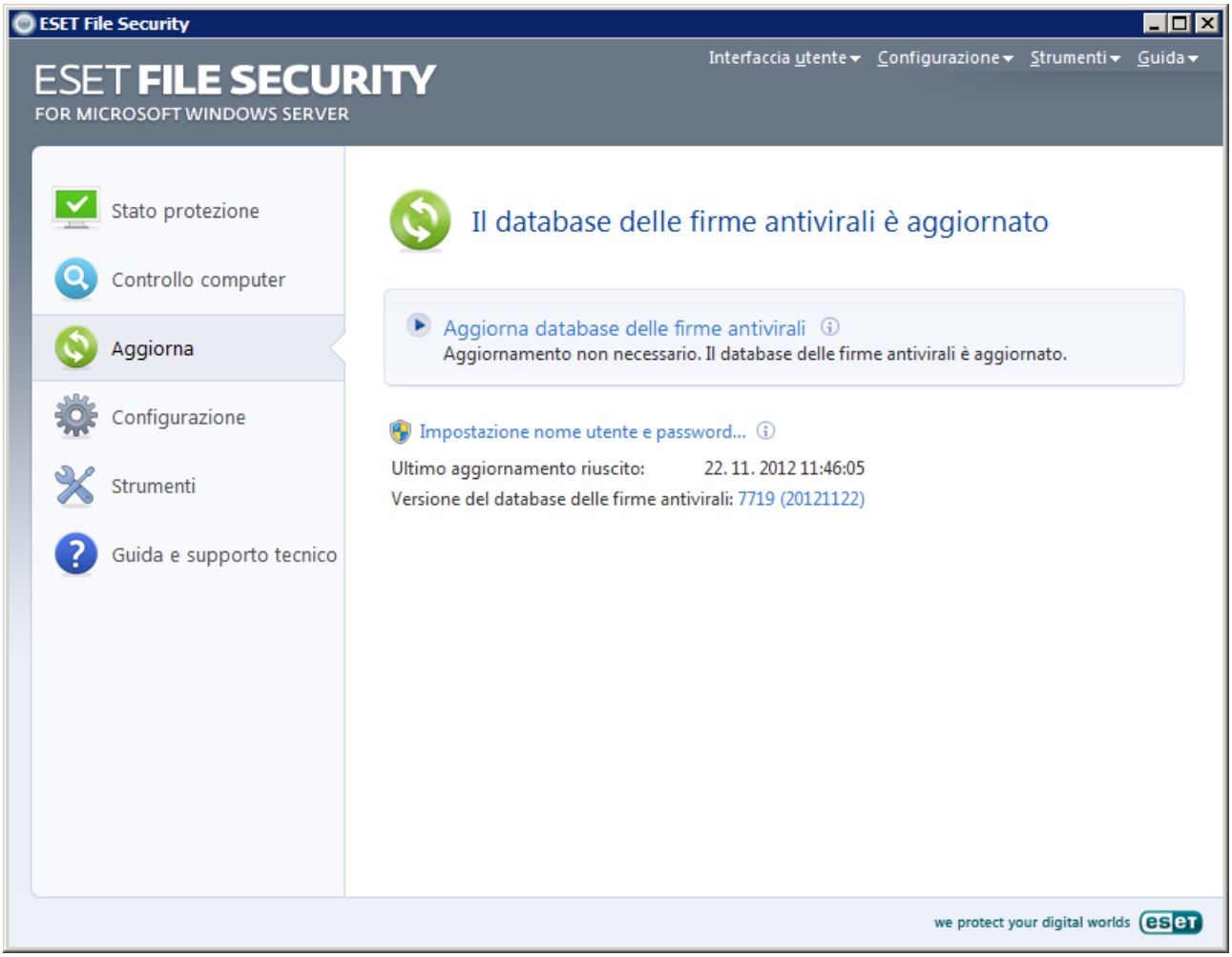
4.3 Aggiornamento del programma

Gli aggiornamenti periodici di ESET File Security rappresentano l'attività di base per ottenere il massimo livello di sicurezza. Il modulo di aggiornamento garantisce in due modi che il programma sia sempre aggiornato: attraverso l'aggiornamento rispettivamente del database delle firme antivirali e dei componenti del sistema.

Facendo clic su **Aggiorna** nel menu principale, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente e valutare se sia necessario un aggiornamento. Nella finestra principale sono inoltre contenute informazioni sulla versione del database delle firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

Inoltre, è disponibile l'opzione per avviare manualmente il processo di aggiornamento (**Aggiorna database delle firme antivirali)**, oltre alle opzioni di base di configurazione dell'aggiornamento, ad esempio il nome utente e la password per accedere ai server di aggiornamento ESET.

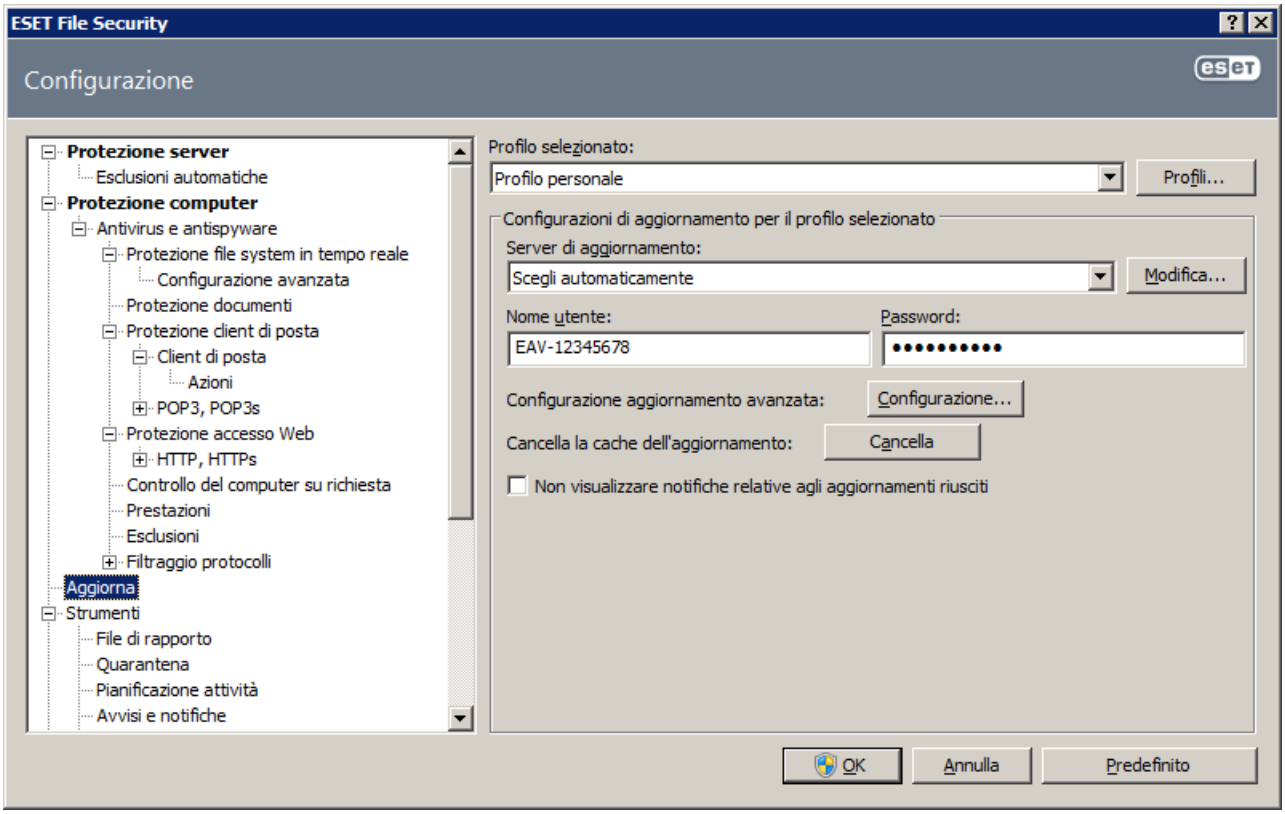
Usare il collegamento **Attivazione prodotto** per accedere al modulo di registrazione che consente di attivare il prodotto di protezione ESET e ricevere un messaggio e-mail contenente i dati per l'autenticazione (nome utente e password).



NOTA: il nome utente e la password vengono forniti da ESET dopo l'acquisto di ESET File Security.

4.3.1 Impostazione aggiornamento

La sezione Configurazione aggiornamento consente di specificare informazioni sull'origine dell'aggiornamento, ad esempio i server di aggiornamento e i dati per l'autenticazione di tali server. Per impostazione predefinita, il menu a discesa **Server di aggiornamento** è impostato su **Scegli automaticamente** per garantire che i file di aggiornamento vengano scaricati automaticamente dal server ESET con meno traffico di rete. Le opzioni di configurazione dell'aggiornamento sono disponibili nella struttura Configurazione avanzata (tasto F5), in **Aggiorna** .

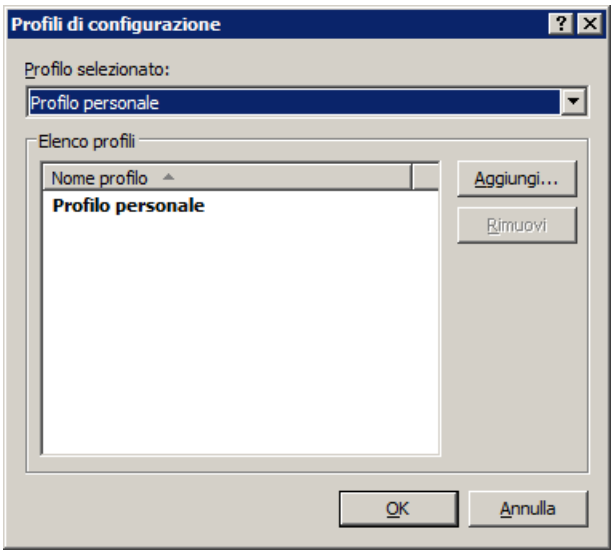


L'elenco dei server di aggiornamento disponibili è accessibile tramite il menu a discesa **Server di aggiornamento**. Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica...** nella sezione **Impostazioni di aggiornamento per il profilo selezionato**, quindi fare clic sul pulsante **Aggiungi**. L'autenticazione per i server di aggiornamento si basa sul **Nome utente** e sulla **Password** generati e inviati dopo aver acquistato il programma.

4.3.1.1 Aggiorna profili

Per varie configurazioni e attività di aggiornamento è possibile creare profili di aggiornamento. La creazione dei profili di aggiornamento è particolarmente utile per gli utenti mobili, i quali possono creare un profilo alternativo per le proprietà di connessione a Internet che cambiano periodicamente.

Nel menu a discesa **Profilo selezionato** è visualizzato il profilo correntemente selezionato, configurato per impostazione predefinita su **Profilo personale**. Per creare un nuovo profilo, fare clic sul pulsante **Profili...**, quindi selezionare il pulsante **Aggiungi...** e immettere il proprio **Nome profilo**. Quando si crea un nuovo profilo, è possibile copiare le impostazioni da uno esistente selezionandolo dal menu a discesa **Copia impostazioni dal profilo**.



Nella finestra di configurazione del profilo è possibile specificare il server di aggiornamento da un elenco di server disponibili oppure aggiungere un nuovo server. L'elenco dei server di aggiornamento esistenti è accessibile tramite il menu a discesa **Server di aggiornamento** . Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica** nella sezione **Impostazioni di aggiornamento per il profilo selezionato**, quindi fare clic sul pulsante **Aggiungi**.

4.3.1.2 Configurazione aggiornamento avanzata

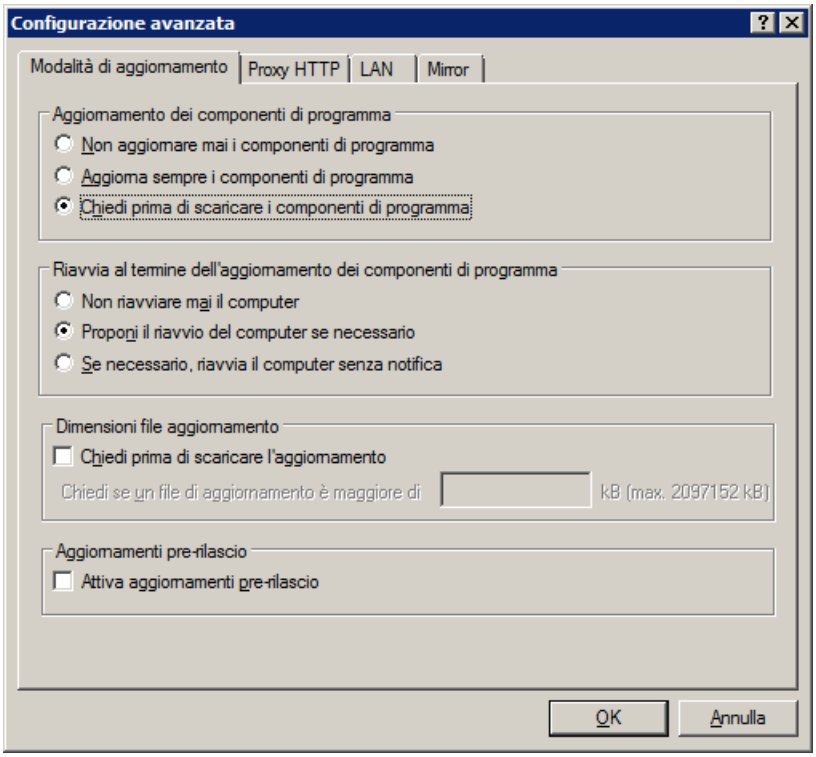
Per visualizzare la configurazione aggiornamento avanzata, fare clic sul pulsante **Configurazione...**. Le opzioni della configurazione aggiornamento avanzata includono la configurazione della **Modalità di aggiornamento**, **Proxy HTTP**, **LAN** e **Mirror**.

4.3.1.2.1 Modalità di aggiornamento

La scheda **Modalità di aggiornamento** contiene opzioni correlate all'aggiornamento dei componenti di programma.

Nella sezione **Aggiornamento componenti programma** sono disponibili tre opzioni:

- **Non aggiornare mai i componenti di programma**: i nuovi componenti di programma non verranno scaricati.
- **Aggiorna sempre i componenti di programma**: i nuovi componenti di programma verranno scaricati automaticamente.
- **Chiedi prima di scaricare i componenti di programma**: opzione predefinita. All'utente verrà chiesto di confermare o rifiutare gli aggiornamenti dei componenti di programma, quando disponibili.


Configurazione avanzata
Modalità di aggiornamento
Proxy HTTP
LAN
Mirror
Aggiornamento dei componenti di programma
Non aggiornare mai i componenti di programma
Aggiorna sempre i componenti di programma
Chiedi prima di scaricare i componenti di programma
Riavvia al termine dell'aggiornamento dei componenti di programma
Non riavviare mai il computer
Proponi il riavvio del computer se necessario
Se necessario, riavvia il computer senza notifica
Dimensioni file aggiornamento
Chiedi prima di scaricare l'aggiornamento
Chiedi se un file di aggiornamento è maggiore di
kB (max. 2097152 kB)
Aggiornamenti pre-rilascio
Attiva aggiornamenti pre-rilascio
OK
Annulla

Dopo aver eseguito un aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer in modo da garantire il corretto funzionamento di tutti i moduli. La sezione **Riavvia dopo l'aggiornamento dei componenti di programma** consente di selezionare una delle opzioni seguenti:

- **Non riavviare mai il computer**
- **Proponi il riavvio del computer se necessario**
- **Se necessario, riavvia il computer senza notifica**

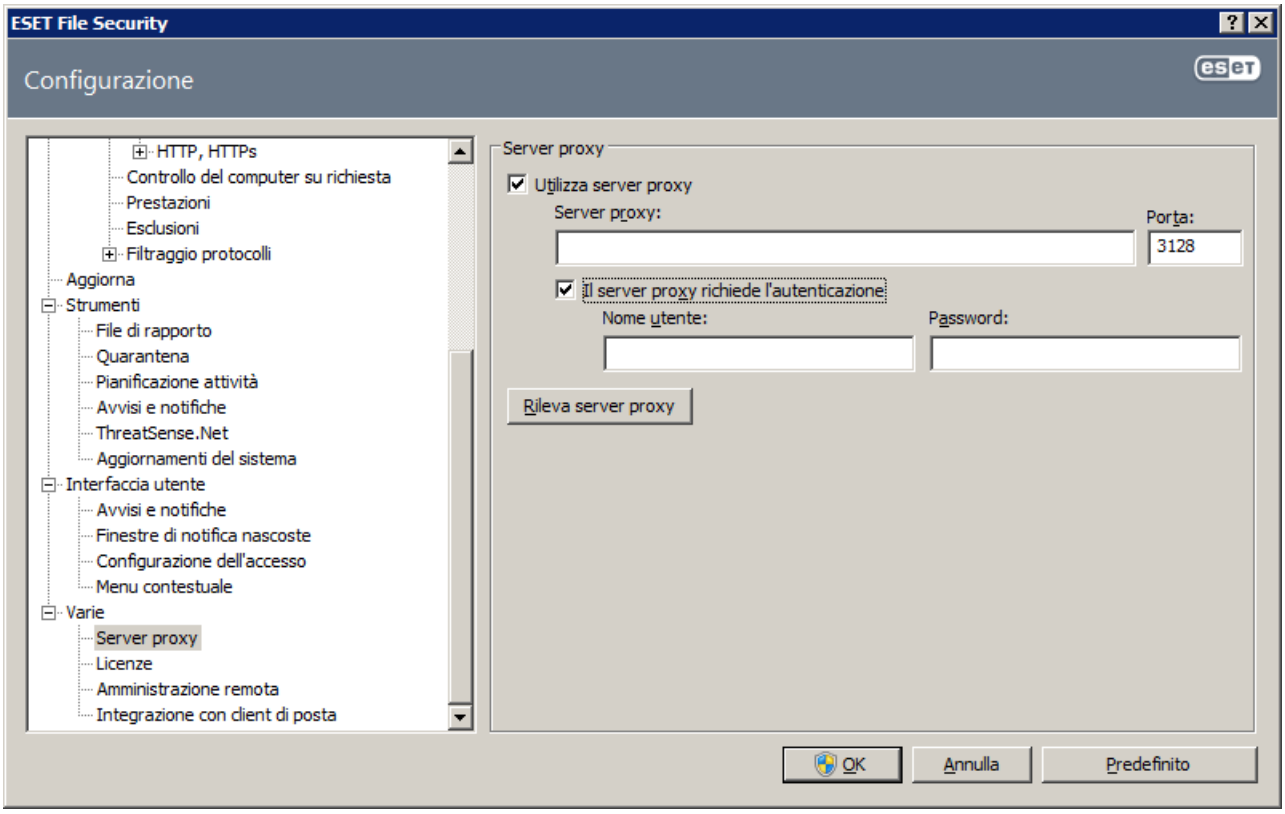
L'opzione predefinita è **Proponi il riavvio del computer se necessario**. La scelta dell'opzione più adatta dipende dalla workstation sulla quale saranno applicate le impostazioni. Tenere presente che esistono alcune differenze tra le workstation e i server. Il riavvio automatico del server dopo un aggiornamento di un componente di programma potrebbe ad esempio causare gravi danni al sistema.

4.3.1.2.2 Server proxy

In ESET File Security, il server proxy può essere configurato in due sezioni differenti della struttura Configurazione avanzata.

Le impostazioni del server proxy possono innanzitutto essere configurate in **Varie** > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per l'intera applicazione ESET File Security. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy a questo livello, selezionare la casella di controllo **Usa server proxy**, quindi immettere l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di **Porta** del server proxy.



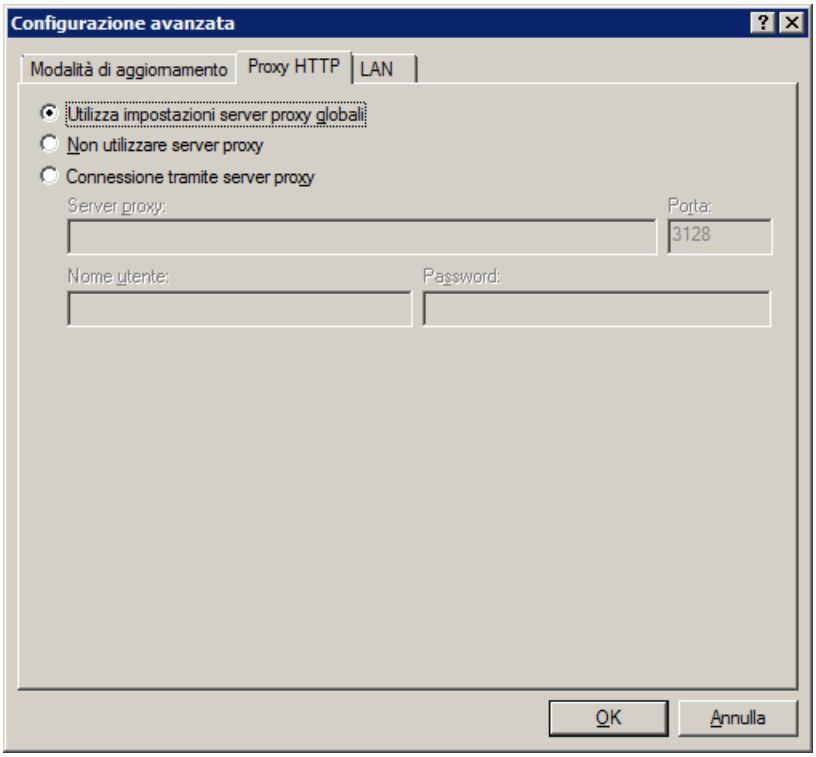
Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare la casella di controllo **Il server proxy richiede l'autenticazione** e immettere **Nome utente** e **Password** validi nei rispettivi campi. Fare clic sul pulsante **Rileva server proxy** per rilevare e inserire automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer.

NOTA: questa funzione non consente di recuperare i dati sull'autenticazione (nome utente e password). Tali informazioni devono quindi essere immesse dall'utente.

Le impostazioni del server proxy possono inoltre essere definite nell'ambito della configurazione aggiornamento avanzata. Questa impostazione è applicabile al profilo di aggiornamento fornito. È possibile accedere alle opzioni di configurazione del server proxy per un determinato profilo di aggiornamento selezionando la scheda **Proxy HTTP** in **Configurazione aggiornamento avanzata**. Sono disponibili le tre seguenti opzioni:

- **Utilizza impostazioni server proxy globali**
- **Non utilizzare server proxy**
- **Connessione tramite server proxy** (connessione definita mediante le proprietà di connessione)

Se si seleziona l'opzione **Utilizza impostazioni server proxy globali**, verranno utilizzate le opzioni di configurazione del server proxy già specificate all'interno della sottostruttura **Varie** > **Server proxy** della struttura Configurazione avanzata (come descritto nella parte iniziale di questo articolo).



Selezionare l'opzione **Non utilizzare server proxy** per specificare che non verrà utilizzato alcun server proxy per l'aggiornamento di ESET File Security.

Selezionare l'opzione **Connessione tramite un server proxy** se si utilizza un server proxy per aggiornare ESET File Security ed è differente da quello specificato nelle impostazioni globali (**Varie** > **Server proxy**). In questo caso, sarà necessario fornire alcune informazioni aggiuntive: Indirizzo del **Server proxy**, **Porta** di comunicazione e **Nome utente** e **Password** del server proxy, se richiesti.

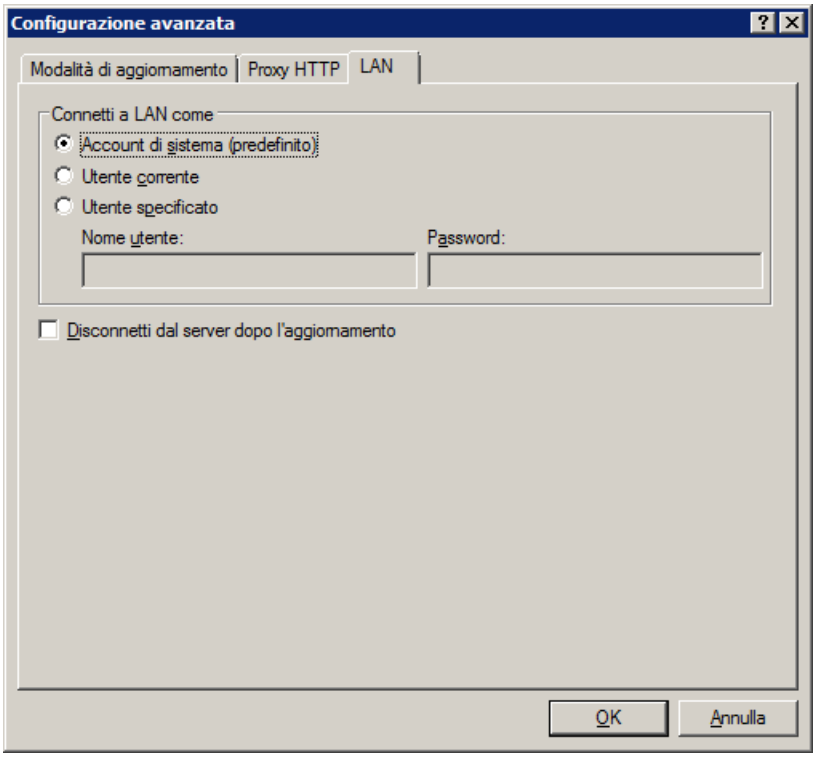
Selezionare questa opzione anche nel caso in cui le impostazioni del server proxy non siano state impostate a livello globale. ESET File Security si connetterà tuttavia a un server proxy per verificare la disponibilità di aggiornamenti.

L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

4.3.1.2.3 Connessione alla LAN

Durante l'aggiornamento da un server locale con un sistema operativo basato su NT, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete. Nella maggior parte dei casi, un account di sistema locale non dispone di diritti di accesso sufficienti per la cartella Mirror (che contiene copie dei file di aggiornamento). In questo caso, immettere nome utente e password nella sezione di configurazione dell'aggiornamento o specificare un account esistente che il programma utilizzerà per accedere al server di aggiornamento (Mirror).

Per configurare tale account, fare clic sulla scheda **LAN**. Nella sezione **Connetti a LAN come** sono disponibili le opzioni **Account di sistema** (**predefinito**), **Utente corrente** e **Utente specificato**.



Selezionare l'opzione **Account di sistema** (**predefinito**) per utilizzare l'account di sistema per l'autenticazione. In genere non viene eseguito alcun processo di autenticazione se nella sezione principale di configurazione dell'aggiornamento non sono specificati dati di autenticazione.

Per essere certi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito correntemente l'accesso, selezionare **Utente corrente**. Lo svantaggio di questa soluzione consiste nel fatto che il programma non è in grado di connettersi al server di aggiornamento se nessun utente ha eseguito correntemente l'accesso.

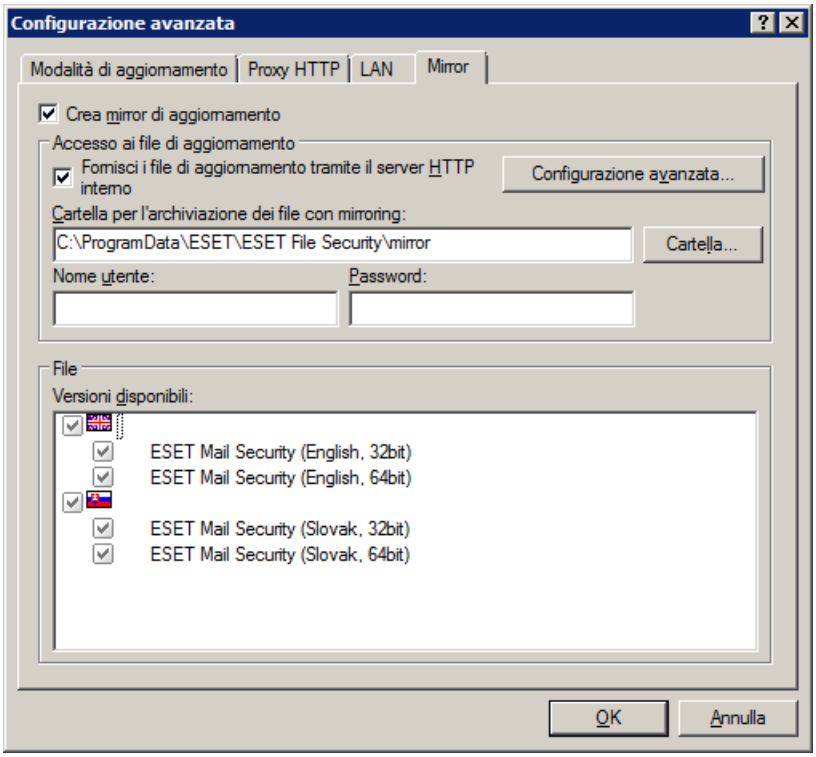
Selezionare **Utente specificato** se si desidera che il programma utilizzi un account utente specifico per l'autenticazione.

Attenzione: se si seleziona **Utente corrente** o **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. È consigliabile inserire i dati di autenticazione della LAN nella sezione principale di configurazione dell'aggiornamento. In questa sezione di configurazione dell'aggiornamento, i dati di autenticazione devono essere inseriti come segue: nome_dominio\utente (se si tratta di un gruppo di lavoro, immettere nome_gruppodilavoro\nome) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

4.3.1.2.4 Creazione di copie di aggiornamento - Mirror

ESET File Security consente di creare copie di file di aggiornamento che è possibile utilizzare per aggiornare altre workstation della rete. L'aggiornamento delle workstation client da un Mirror consente di ottimizzare il bilanciamento del carico di rete e di risparmiare ampiezza di banda per la connessione a Internet.

Le opzioni di configurazione per il server Mirror locale sono accessibili (dopo aver aggiunto una chiave di licenza valida nella gestione licenze nella sezione Configurazione avanzata di ESET File Security) nella sezione **Configurazione aggiornamento avanzata** . Per accedere a questa sezione, premere F5 e fare clic su **Aggiorna** nella struttura Configurazione avanzata, quindi selezionare il pulsante **Configurazione...** accanto a **Configurazione aggiornamento avanzata** e selezionare la scheda **Mirror**).



Il primo passaggio della procedura di configurazione del Mirror consiste nel selezionare l'opzione Crea mirror di aggiornamento. Selezionando questa opzione vengono attivate altre opzioni di configurazione del Mirror come la modalità di accesso ai file di aggiornamento e il percorso di aggiornamento per i file con mirroring.

I metodi di attivazione del Mirroring sono descritti in dettaglio nella sezione Aggiornamento dal Mirror. Per il momento, tenere presente che sono disponibili due metodi di base per l'accesso al Mirror: la cartella con i file di aggiornamento può essere presentata come una cartella di rete condivisa o come un server HTTP.

La cartella dedicata alla memorizzazione dei file di aggiornamento per il Mirror è definita nella sezione **Cartella per l'archiviazione dei file con mirroring**. Fare clic su **Cartella...** per cercare una cartella sul computer locale o sulla cartella di rete condivisa. Se è necessaria l'autorizzazione per la cartella specificata, i dati di autenticazione devono essere specificati nei campi **Nome utente** e **Password**. Nome utente e Password devono essere specificati nel formato *Dominio/Utente* o *Gruppo di lavoro/Utente*. È necessario specificare le password corrispondenti.

Quando si configura il Mirror, è anche possibile specificare le versioni della lingua per le quali si desidera scaricare le copie di aggiornamento. L'impostazione della versione della lingua è disponibile nella sezione **File** - **Versioni disponibili**:.

4.3.1.2.4.1 Aggiornamento dal Mirror

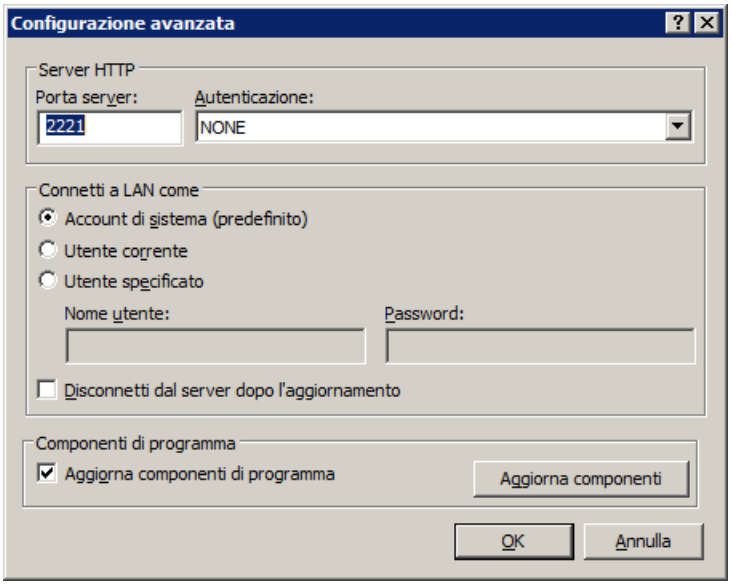
Sono disponibili due metodi di base per la configurazione del mirror: la cartella con i file di aggiornamento può essere presentata come una cartella di rete condivisa o come un server HTTP.

Accesso al Mirror mediante un server HTTP interno

Questa rappresenta la configurazione predefinita specificata nella configurazione originale del programma. Per consentire l'accesso al Mirror tramite il server HTTP, accedere alla sezione **Configurazione aggiornamento avanzata** (scheda **Mirror**) e selezionare l'opzione **Crea mirror di aggiornamento**.

Nella sezione **Configurazione avanzata** della scheda **Mirror** è possibile specificare la **Porta server** di ascolto del server HTTP, oltre al tipo di **Autenticazione** utilizzata dal server HTTP. Per impostazione predefinita, la porta server è configurata su **2221**. L'opzione **Autenticazione** definisce il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **NESSUNO**, **Base** ed **NTLM**. Selezionare **Base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password. L'opzione **NTLM** consente l'uso di un metodo di codifica sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation di condivisione dei file di aggiornamento. L'impostazione predefinita è **NESSUNO**, che consente l'accesso ai file di aggiornamento senza che sia necessaria l'autenticazione.

Attenzione: se si desidera consentire l'accesso ai file di aggiornamento tramite il server HTTP, la cartella Mirror deve essere posizionata sullo stesso computer dell'istanza di ESET File Security che la crea.



Al termine della configurazione del Mirror, accedere alle workstation e aggiungere un nuovo server di aggiornamento nel formato **http://indirizzo_IP_del_server:2221**. Per eseguire questa operazione, effettuare i seguenti passaggi:

- Aprire la **Configurazione avanzata di ESET File Security** e fare clic sulla sottostruttura **Aggiorna**.
- Fare clic su **Modifica...** a destra del menu a discesa **Server di aggiornamento** e aggiungere un nuovo server usando il seguente formato: http://Indirizzo_IP_del_server:2221.
- Selezionare il server appena aggiunto dall'elenco di server di aggiornamento.

Accesso al Mirror tramite le condivisioni di sistema

È innanzitutto necessario creare una cartella condivisa su un dispositivo locale o di rete. Durante la creazione della cartella per il Mirror, è necessario garantire l'accesso in scrittura all'utente che salverà i file nella cartella e l'accesso in lettura a tutti gli utenti che aggiorneranno ESET File Security dalla cartella Mirror.

Configurare quindi l'accesso al Mirror nella sezione **Configurazione aggiornamento avanzata** (scheda **Mirror**) disattivando l'opzione **Fornisci i file di aggiornamento tramite il server HTTP interno**. Questa opzione è attivata per impostazione predefinita nel pacchetto di installazione del programma.

Se la cartella condivisa è posizionata su un altro computer della rete, sarà necessario specificare i dati di autenticazione per l'accesso all'altro computer. Per specificare i dati di autenticazione, aprire Configurazione avanzata di ESET File Security (F5) e selezionare **Aggiorna**. Fare clic sul pulsante **Configurazione...**, quindi

selezionare la scheda **LAN**. Questa impostazione è la stessa anche per l'aggiornamento, come illustrato nella sezione Connessione alla LAN.

Una volta completata la configurazione del Mirror, accedere alle workstation e impostare \\UNC\PATH come server di aggiornamento. Questa operazione può essere completata effettuando i passaggi riportati di seguito:

- Aprire Configurazione avanzata di ESET File Security e selezionare **Aggiorna**
- Fare clic su **Modifica...** accanto a Serve di aggiornamento e aggiungere un nuovo server utilizzando il *formato* \ *UNC**PATH*.
- Selezionare il server appena aggiunto dall'elenco di server di aggiornamento.

NOTA: per un corretto funzionamento, il percorso alla cartella Mirror deve essere specificato come percorso UNC. Gli aggiornamenti dalle unità mappate potrebbero non funzionare.

4.3.1.2.4.2 Risoluzione dei problemi di aggiornamento Mirror

Nella maggior parte dei casi, i problemi durante un aggiornamento da un server Mirror sono causati da uno o più dei seguenti motivi: specifica non corretta delle opzioni della cartella Mirror, autenticazione non corretta dei dati nella cartella Mirror, configurazione non corretta sulle workstation locali che tentano di scaricare i file di aggiornamento dal Mirror o una combinazione di questi motivi. Di seguito viene riportata una panoramica sui problemi più frequenti che potrebbero verificarsi durante un aggiornamento dal Mirror:

ESET File Security **riporta un errore di connessione al server Mirror** - Probabilmente causato da una specifica non corretta del server di aggiornamento (percorso di rete alla cartella Mirror) dal quale le workstation locali scaricano gli aggiornamenti. Per verificare la cartella, selezionare il menu **Start** di Windows, fare clic su **Esegui**, inserire il nome della cartella e selezionare **OK**. Dovrebbe essere visualizzato il contenuto della cartella.

ESET File Security **richiede un nome utente e una password** - Probabilmente causato dall'immissione non corretta dei dati di autenticazione (nome utente e password) nella sezione di aggiornamento.. Il nome utente e la password sono utilizzati per concedere l'accesso al server di aggiornamento dal quale il programma si aggiornerà. Verificare che i dati di autenticazione siano corretti e immessi nel formato appropriato. Ad esempio, *Dominio/Nome utente* o *Gruppo di lavoro/Nome utente*, oltre alle password corrispondenti. Se il server Mirror è accessibile a "Tutti", non significa l'accesso è concesso a qualsiasi utente. Con "Tutti" non si intendono utenti non autorizzati. Si intende solo che la cartella è accessibile a tutti gli utenti del dominio. Di conseguenza, se una cartella è accessibile a "Tutti", sarà comunque necessario specificare un nome utente di dominio e una password nella sezione di impostazione dell'aggiornamento.

ESET File Security **riporta un errore di connessione al server Mirror** - La comunicazione sulla porta definita per l'accesso alla versione HTTP del Mirror è bloccata.

4.3.2 Come creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra principale visualizzata dopo aver selezionato l'opzione Aggiorna dal menu principale.

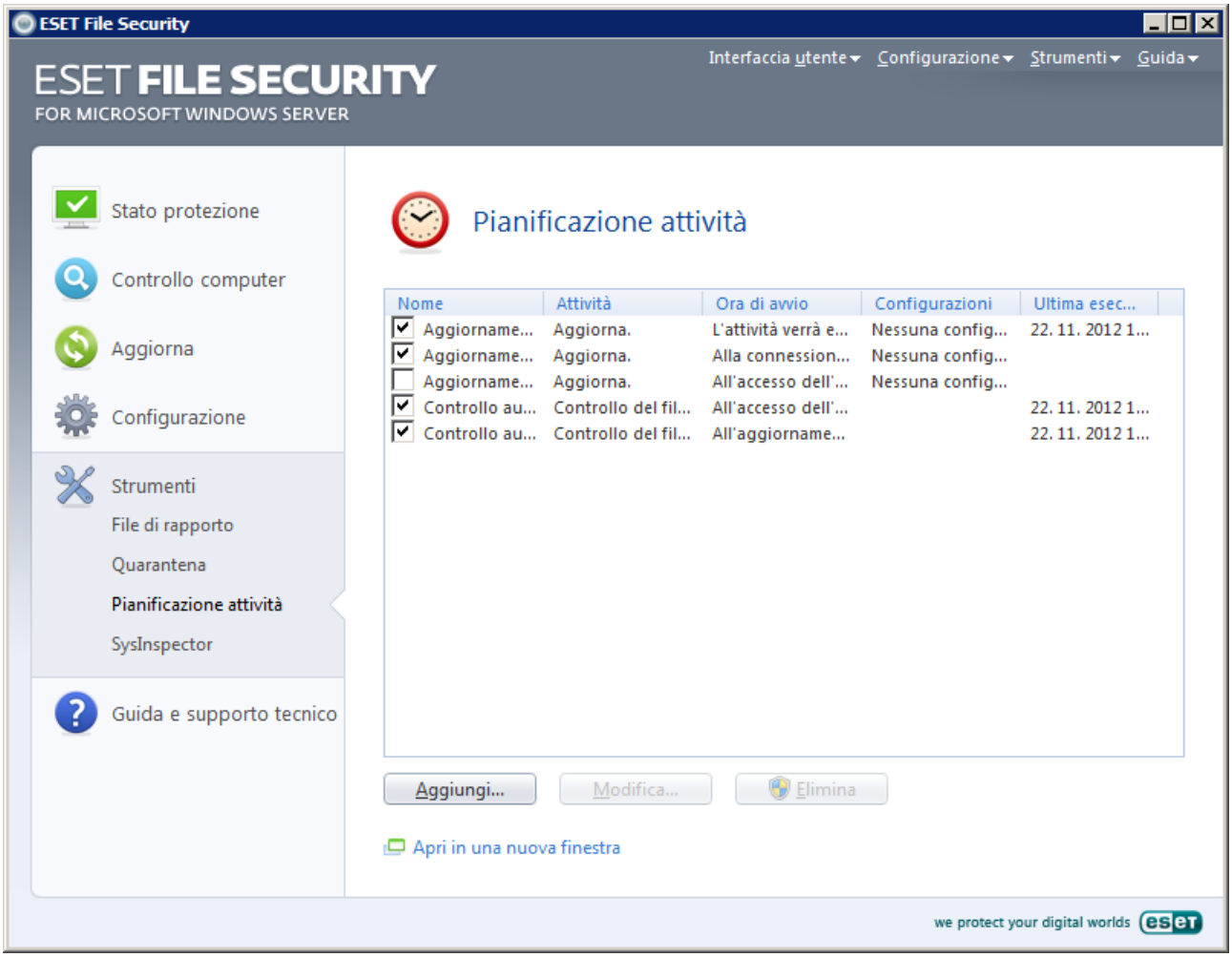
Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET File Security sono attivate le seguenti attività:

- **Aggiornamento automatico periodico**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna delle attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, consultare la sezione Pianificazione attività.

4.4 Pianificazione attività

La funzione Pianificazione attività è disponibile se la modalità avanzata in ESET File Security è attivata. È possibile accedere a **Pianificazione attività** nel menu principale di ESET File Security in **Strumenti**. La Pianificazione attività contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, ad esempio data, ora e profilo di controllo predefiniti utilizzati.



Per impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Aggiornamento automatico periodico**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controllo automatico file di avvio (dopo l'accesso utente)**
- **Controllo automatico file di avvio (dopo il completamento dell'aggiornamento del database delle firme antivirali)**

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività e selezionare **Modifica...** oppure selezionare l'attività che si desidera modificare e fare clic sul pulsante **Modifica...**.

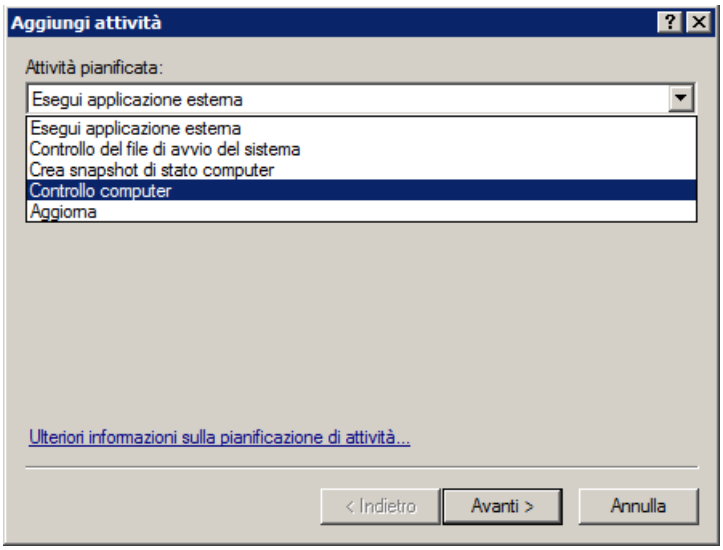
4.4.1 Scopo della pianificazione delle attività

La Pianificazione attività consente di gestire e avviare attività pianificate con configurazione e proprietà predefinite. La configurazione e le proprietà contengono informazioni quali la data e l'ora, oltre a profili specifici da utilizzare durante l'esecuzione dell'attività.

4.4.2 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi...** oppure fare clic con il tasto destro del mouse e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna**
- **Controllo del file di avvio del sistema**
- **Crea snapshot di stato computer**
- **Controllo del computer su richiesta**
- **Aggiorna**



Poiché **Aggiorna** rappresenta una delle attività pianificate utilizzata con maggiore frequenza, verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento.

Nel menu a discesa **Attività pianificata**:, selezionare **Aggiorna**. Fare clic su **Avanti** e immettere il nome dell'attività nel campo **Nome attività** . Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

- **Attendi il successivo intervallo pianificato**
- **Esegui l'attività appena possibile**
- **Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato** (t possibile definire l'intervallo utilizzando la casella di scorrimento Intervallo attività)

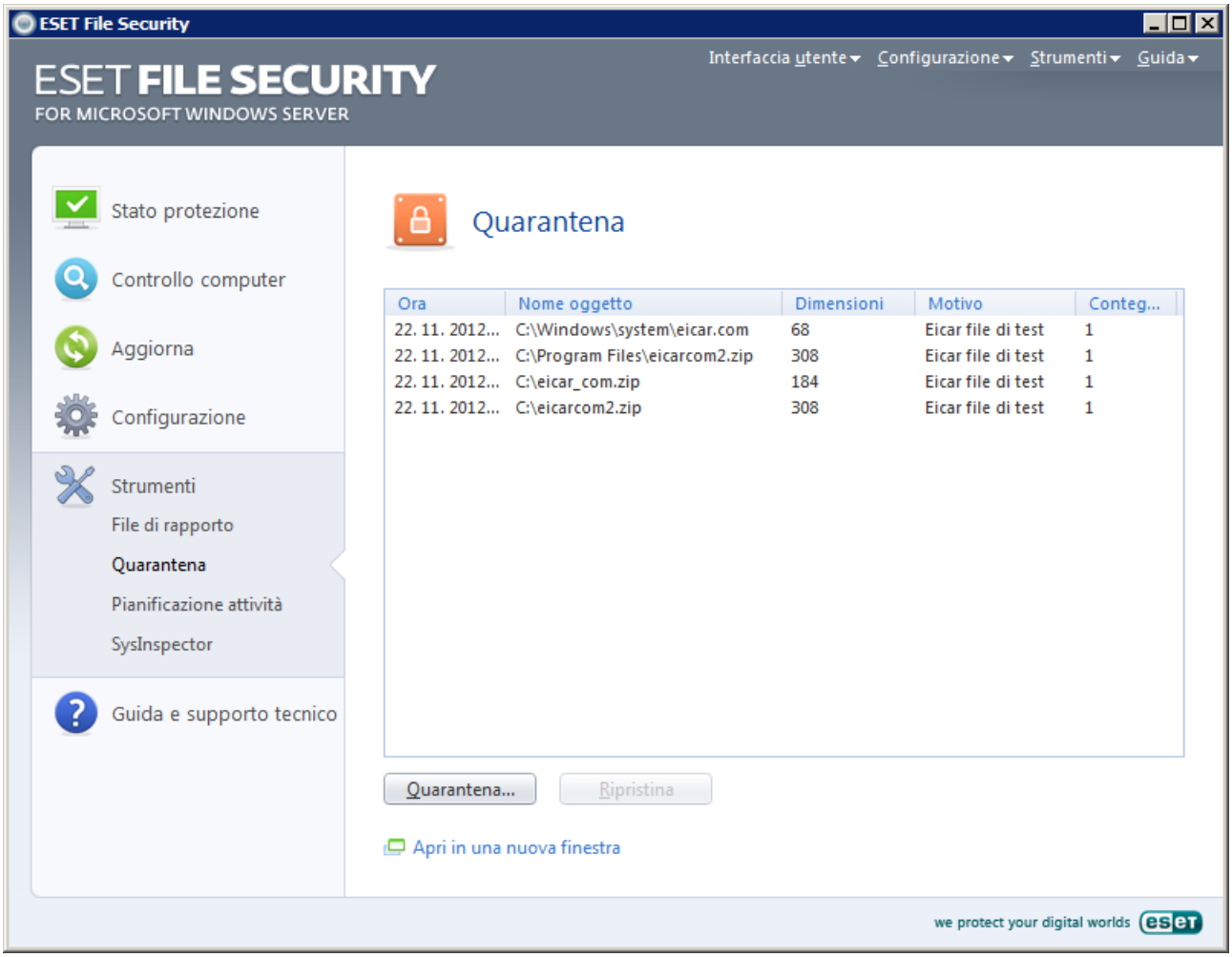
Nel passaggio successivo, viene visualizzata una finestra contenente un riepilogo delle informazioni sull'attività pianificata corrente; l'opzione **Esegui attività con i parametri specificati** dovrebbe essere automaticamente abilitata. Fare clic sul pulsante **Fine**.

Verrà visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui è possibile indicare un profilo principale e uno alternativo, da utilizzare nel caso in cui l'attività non possa essere completata con il profilo principale. Confermare facendo clic su **OK** nella finestra **Aggiorna profili**. La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

4.5 Quarantena

Lo scopo principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET File Security.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati ai laboratori antivirus ESET per l'analisi.



I file salvati nella cartella di quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio **aggiunto dall'utente...**), e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni).

4.5.1 Mettere file in quarantena

ESET File Security mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto ad annullare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando il pulsante **Quarantena**. In tal caso, il file originale non viene rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare l'opzione **Aggiungi...**.

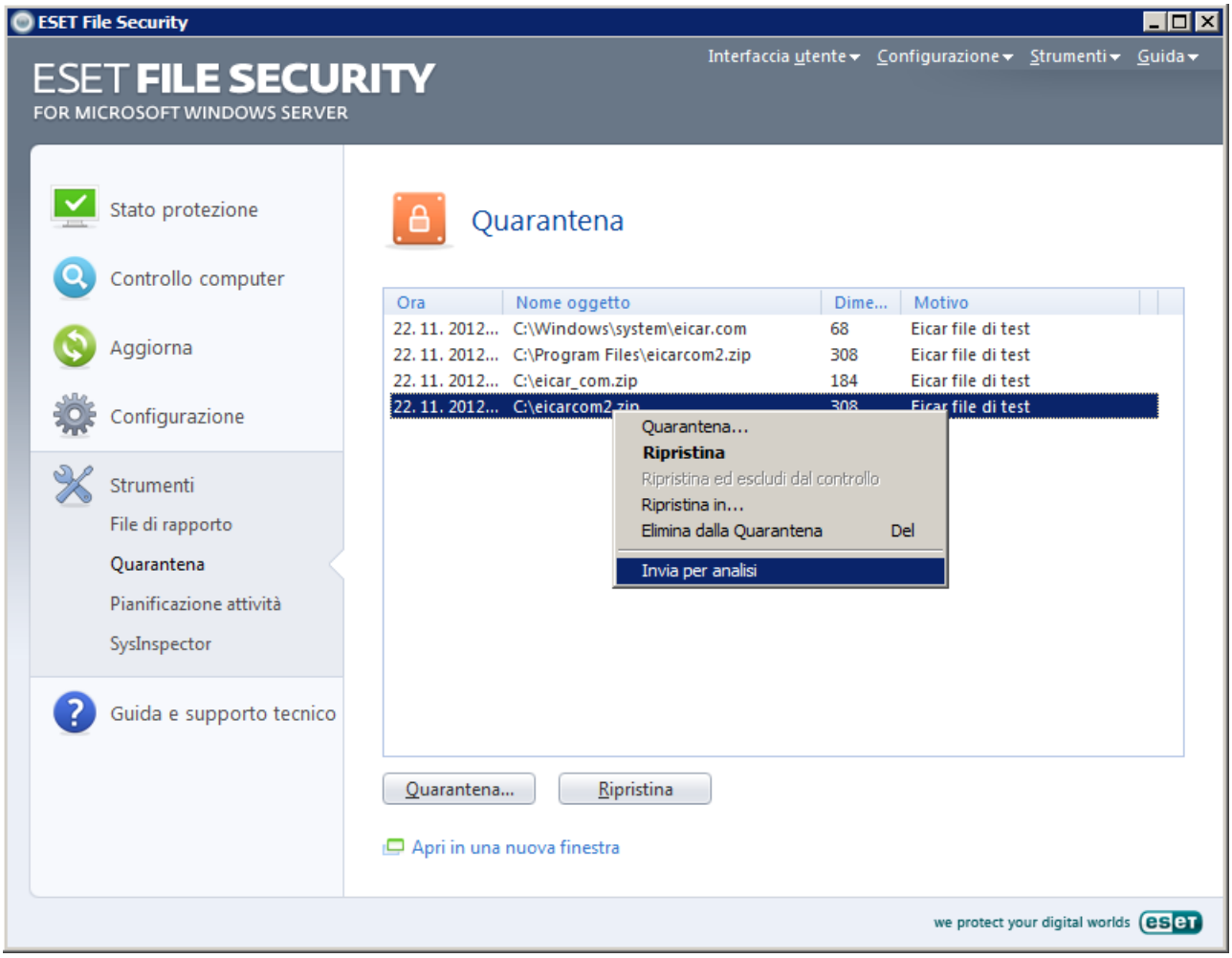
4.5.2 Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. A tale scopo, utilizzare la funzione **Ripristina**, disponibile nel menu contestuale visualizzato facendo clic con il pulsante destro del mouse sul file desiderato nella finestra Quarantena. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

NOTA: se il programma ha messo in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

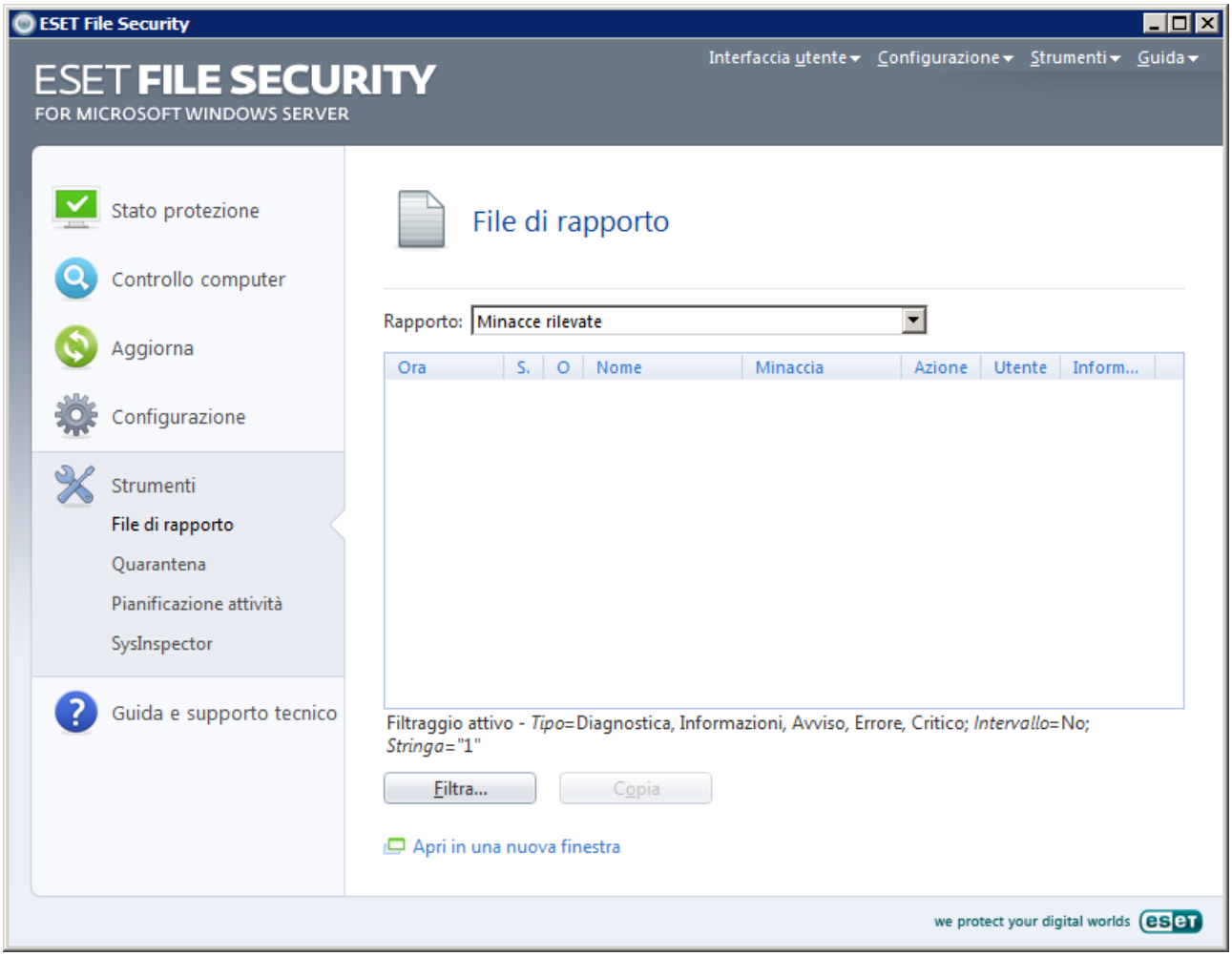
4.5.3 Invio di file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena, o se un file è stato valutato erroneamente come infetto (ad esempio da un'analisi euristica del codice) e quindi messo in quarantena, inviare il file ai laboratori antivirus ESET. Per inviare un file dalla cartella di quarantena, fare clic con il pulsante destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.



4.6 File di rapporto

I file di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta uno strumento essenziale per l'analisi del sistema, il rilevamento delle minacce e la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET File Security.



È possibile accedere ai file di rapporto dal menu principale facendo clic su **Strumenti** > **File di rapporto**. Selezionare il tipo di rapporto desiderato nel menu a discesa **Rapporto** nella parte superiore della finestra. Sono disponibili i rapporti seguenti:

- **Minacce rilevate** - Utilizzare questa opzione per visualizzare tutte le informazioni sugli eventi correlate alle infiltrazioni rilevate, ad eccezione delle infiltrazioni rilevate dal controllo del computer su richiesta (questi eventi vengono registrati nel rapporto **Controllo computer su richiesta**).
- **Eventi** - Questa opzione è utile agli amministratori di sistema e agli utenti per risolvere i problemi. Tutte le azioni importanti eseguite da ESET File Security vengono registrate nei rapporti degli eventi.
- **Controllo computer su richiesta** - In questa finestra vengono visualizzati i risultati di tutti i controlli completati. Fare doppio clic su una voce per visualizzare i dettagli del rispettivo controllo su richiesta.

In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti selezionando la voce desiderata e facendo clic sul pulsante **Copia**. Per selezionare più voci, usare i tasti CTRL e MAIUSC.

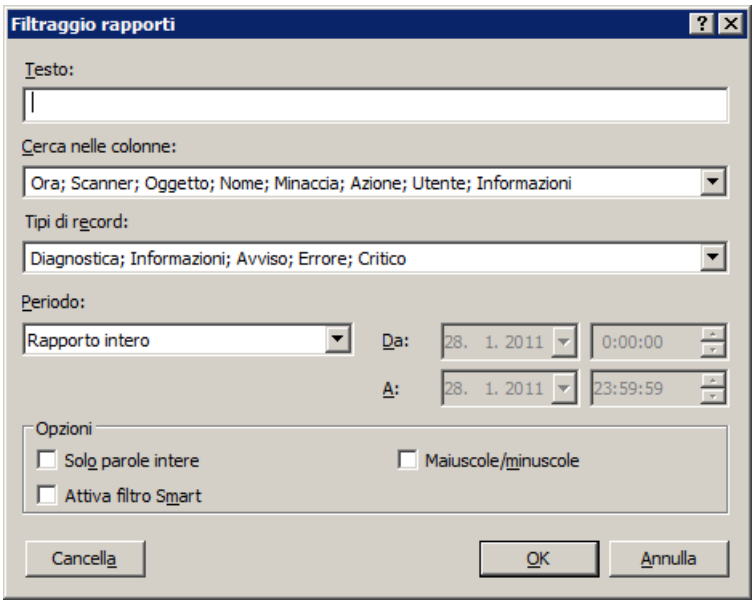
4.6.1 Filtraggio rapporti

La funzione Filtraggio rapporti aiuta a trovare i record nei file di rapporto, soprattutto se è presente un numero elevato di record ed è difficile trovare le informazioni specifiche necessarie.

Se si utilizza la funzione di filtraggio, è possibile immettere una stringa di **Cosa** filtrare, specificare le **colonne in cui eseguire la ricerca**, selezionare **Tipi di record** e impostare un **Periodo** per restringere il numero di record. Specificando alcune opzioni di filtraggio, nella finestra **File di rapporto** vengono visualizzati solo i record pertinenti, in base alle opzioni di filtraggio, al fine di facilitare e velocizzare l'accesso.

Per aprire la finestra **Filtraggio rapporti**, premere il pulsante **Filtra...** in **Strumenti** > **File di rapporto**, oppure utilizzare i tasti di scelta rapida Ctrl + Alt + F.

NOTA: per ricercare un record specifico, è possibile utilizzare la funzione Trova nel rapporto singolarmente o insieme alla funzione Filtraggio rapporti.



Specificando alcune opzioni di filtraggio, nella finestra File di rapporto vengono visualizzati solo i record pertinenti in base alle opzioni di filtraggio. I record verranno filtrati/ristretti, facilitando la ricerca. Maggiore è la specificità delle opzioni di filtraggio utilizzate, più ristretto sarà il risultato restituito.

Cosa: - Digitare una stringa (parola o parte di una parola). Verranno visualizzati solo i record contenenti tale stringa. I restanti record non saranno visibili per facilitare la lettura.

Cerca nelle colonne: - Selezionare le colonne in cui applicare il filtraggio. È possibile selezionare una o più colonne da utilizzare per il filtraggio. Per impostazione predefinita, sono selezionate tutte le colonne:

- **Ora**
- **Modulo**
- **Evento**
- **Utente**

Tipi di record: - Consente di scegliere i tipi di record da visualizzare. È possibile scegliere un tipo di record particolare, più tipi di record contemporaneamente o visualizzare tutti i tipi di record (impostazione predefinita):

- **Diagnostica**
- **Informazioni**
- **Attenzione**
- **Errore**
- **Critico**

Periodo: - Utilizzare questa opzione per filtrare i record in base a un periodo specifico. Sono disponibili le seguenti opzioni:

- **Rapporto intero** (impostazione predefinita) - Il filtraggio non viene eseguito nel periodo indicato poiché viene visualizzato l'intero rapporto
- **Ultimo giorno**
- **Ultima settimana**
- **Ultimo mese**
- **Intervallo** - Se si seleziona questa opzione, è possibile specificare il periodo esatto (data e ora) per visualizzare solo i record che si sono verificati nel periodo specificato.

Oltre alle precedenti impostazioni di filtraggio, sono disponibili anche alcune **Opzioni**:

Solo parole intere - Visualizza solo i record contenenti una stringa corrispondente alla parola intera nella casella di testo **Cosa**.

Maiuscole/minuscole - Visualizza solo i record contenenti una stringa corrispondente al formato maiuscolo/minuscolo nella casella di testo **Cosa**.

Attiva filtro Smart - Utilizzare questa opzione per consentire a ESET File Security di eseguire il filtraggio utilizzando i propri metodi.

Al termine della configurazione delle opzioni di filtraggio, premere il pulsante **OK** per applicare il filtro. Nella finestra **File di rapporto** verranno visualizzati solo i record corrispondenti in base alle opzioni di filtraggio.

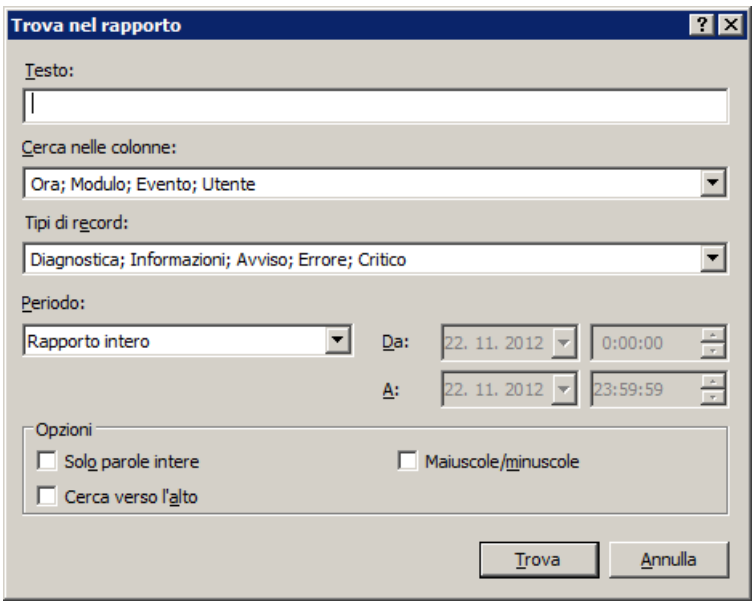
4.6.2 Trova nel rapporto

Oltre alla funzione Filtraggio dei rapporti, è possibile utilizzare la funzionalità di ricerca all'interno dei file di rapporto che può essere utilizzata indipendentemente dal filtraggio dei rapporti. Si tratta di una funzionalità utile se si desidera ricercare particolari record nei rapporti. Al pari del Filtraggio rapporti, questa funzionalità di ricerca aiuta a trovare le informazioni che si stanno ricercando, soprattutto se è presente un numero elevato di record.

Se si utilizza la funzione Trova nel rapporto, è possibile immettere una stringa di **Cosa** filtrare, specificare le **colonne in cui eseguire la ricerca**, selezionare **Tipi di record** e impostare un **Periodo** per ricercare solo i record verificati nel periodo indicato. Specificando alcune opzioni di ricerca, nella finestra File di rapporto vengono visualizzati solo i record pertinenti in base alle opzioni di ricerca.

Per eseguire la ricerca nei rapporti, premere i tasti Ctrl + f per aprire la finestra **Trova nel rapporto**.

NOTA: la funzione Trova nel rapporto può essere utilizzata insieme alla funzione Filtraggio rapporti. È prima possibile restringere il numero di record utilizzando la funzione Filtraggio rapporto e iniziare quindi la ricerca solo nei record filtrati.



Cosa: - Digitare una stringa (parola o parte di una parola). Verranno trovati solo i record contenenti tale stringa. I restanti record verranno omessi.

Cerca nelle colonne: - Selezionare le colonne in cui eseguire la ricerca. È possibile selezionare una o più colonne da utilizzare per la ricerca. Per impostazione predefinita, sono selezionate tutte le colonne:

- **Ora**
- **Modulo**
- **Evento**
- **Utente**

Tipi di record: - Consente di scegliere i tipi di record da trovare. È possibile scegliere un tipo di record particolare, più tipi di record contemporaneamente o ricercare tutti i tipi di record (impostazione predefinita):

- **Diagnostica**
- **Informazioni**
- **Attenzione**
- **Errore**
- **Critico**

Periodo: - Utilizzare questa opzione per trovare i record solo all'interno di un periodo specifico. Sono disponibili le seguenti opzioni:

- **Rapporto intero** (impostazione predefinita) - La ricerca non viene eseguita nel periodo indicato ma nell'intero rapporto
- **Ultimo giorno**
- **Ultima settimana**
- **Ultimo mese**
- **Intervallo** - Se si seleziona questa opzione, è possibile specificare il periodo esatto (data e ora) per ricercare solo i record che si sono verificati nel periodo specificato.

Oltre alle precedenti impostazioni di ricerca, sono disponibili anche alcune **Opzioni**:

Solo parole intere - Trova solo i record contenenti una stringa corrispondente alla parola intera nella casella di testo **Cosa**.

Maiuscole/minuscole - Trova solo i record contenenti una stringa corrispondente al formato maiuscolo/minuscolo nella casella di testo **Cosa**.

Cerca verso l'alto - La ricerca viene eseguita dalla posizione corrente verso l'alto.

Dopo aver configurato le opzioni di ricerca, fare clic sul pulsante **Trova** per iniziare la ricerca. La ricerca si interrompe quando viene trovato il primo record corrispondente. Fare nuovamente clic sul pulsante **Trova** per proseguire ulteriormente la ricerca. La ricerca nei file di rapporto viene eseguita dall'alto verso il basso, partendo dalla posizione corrente, ovvero dal record evidenziato.

4.6.3 Manutenzione rapporto

La configurazione della registrazione di ESET File Security è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Immetti struttura di configurazione avanzata completa...** > **Strumenti** > **File di rapporto**. Per i file di rapporto è possibile specificare le opzioni seguenti:

- **Elimina record automaticamente**: Le voci del rapporto più vecchie del numero specificato di giorni verranno eliminate automaticamente
- **Ottimizza automaticamente file di rapporto**: Consente la deframmentazione automatica dei file di rapporto se si supera la percentuale specificata di record inutilizzati
- **Livello minimo di dettaglio del rapporto**: Consente di specificare il livello minimo di dettaglio del rapporto. Opzioni disponibili:

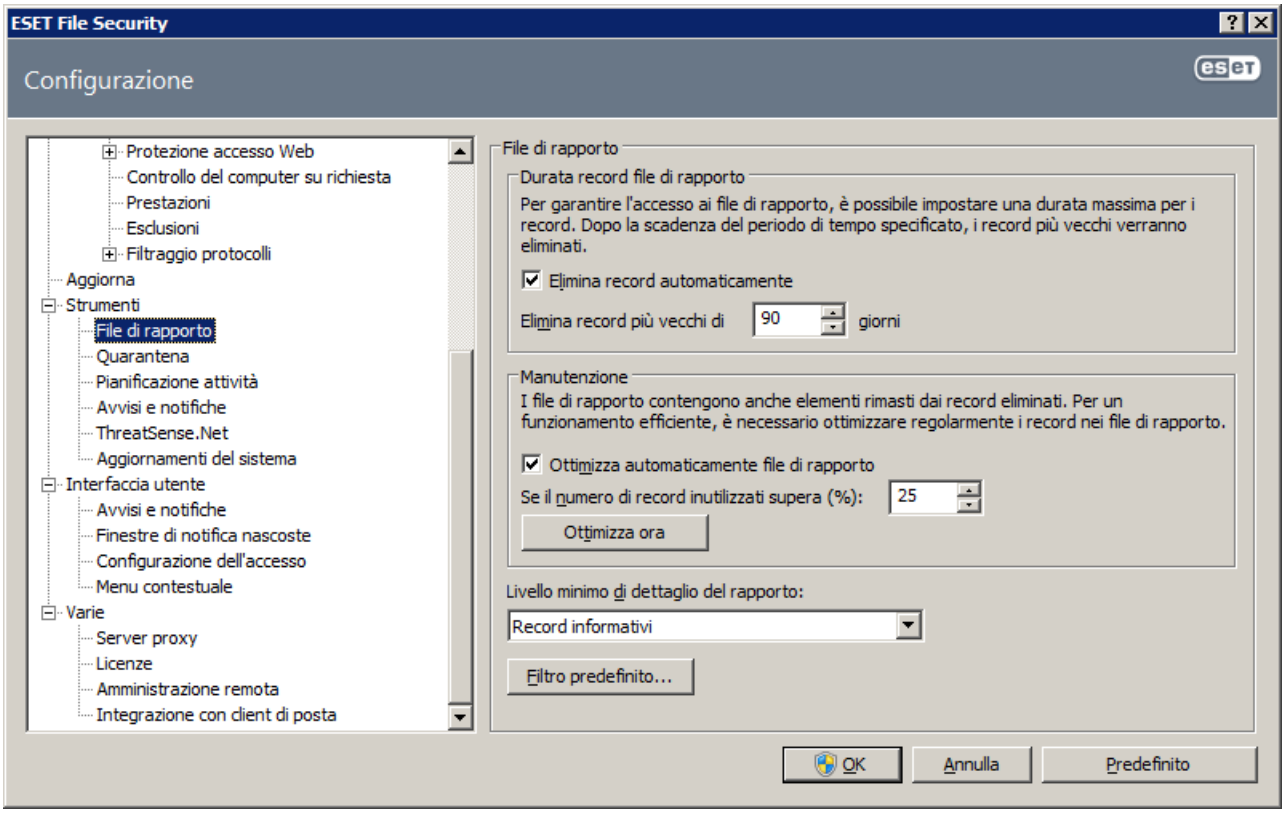
- **Record di diagnostica** - Consente di registrare tutte le informazioni necessarie per ottimizzare il programma e tutti i record precedenti

- **Record informativi** - Messaggi di record informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza

- **Avvisi** - Consente di registrare errori critici e messaggi di allarme

- **Errori** - Verranno registrati solo errori quali "Errore durante il download del file" ed errori critici

- **Avvisi Critici** - Registra solo gli errori critici (errore che avvia la protezione antivirus e così via)



4.7 ESET SysInspector

4.7.1 Introduzione a ESET SysInspector

L'applicazione ESET SysInspector ispeziona il computer in modo approfondito e visualizza i dati raccolti in modo esauriente. La raccolta di informazioni su driver e applicazioni installati, connessioni di rete o importanti voci di registro semplifica il controllo di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

È possibile accedere a ESET SysInspector in due modi: dalla versione integrata nelle soluzioni ESET Security o scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web ESET. Le funzionalità e i comandi di entrambe le versioni sono identici. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono entrambe di esportare snapshot del sistema su un file *XML* e salvarli su disco. La versione integrata consente tuttavia anche di memorizzare gli snapshot di sistema direttamente in **Strumenti** > **ESET SysInspector** (tranne ESET Remote Administrator). Per ulteriori informazioni, vedere la sezione ESET SysInspector come componente di ESET File Security.

È necessario attendere qualche minuto per consentire a ESET SysInspector di controllare il computer. A seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate nel computer in uso, questa operazione potrebbe richiedere da 10 secondi ad alcuni minuti.

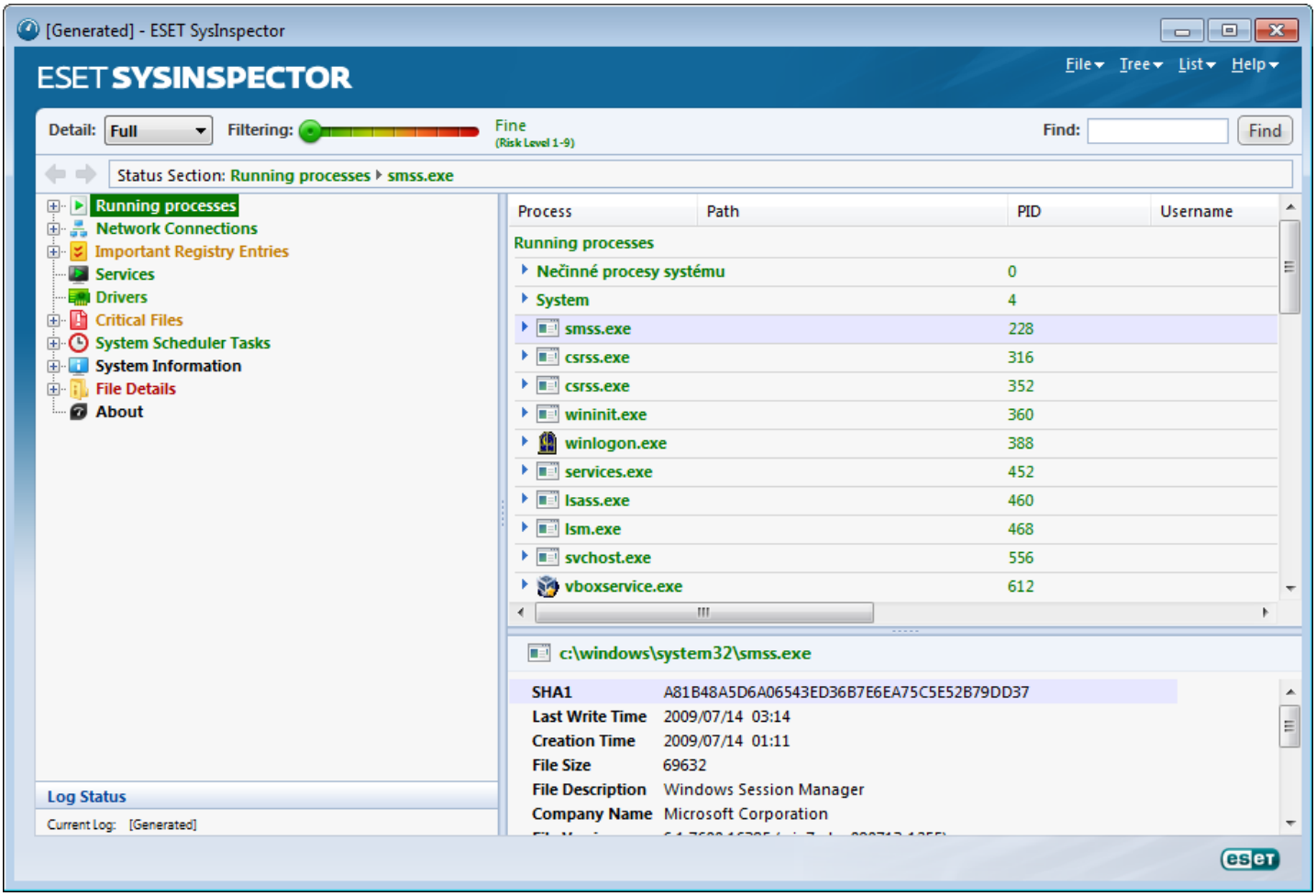
4.7.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector è sufficiente eseguire il file eseguibile *SysInspector.exe* scaricato dal sito Web ESET. Se è già installata una delle soluzioni ESET Security, è possibile eseguire ESET SysInspector direttamente dal menu Start (**Programmi** > **ESET** > **ESET File Security**).

È necessario attendere che l'applicazione abbia esaminato il sistema in uso. Questa operazione potrebbe richiedere diversi minuti a seconda dell'hardware e dei dati raccolti.

4.7.2 Interfaccia utente e utilizzo dell'applicazione

Per chiarezza, la finestra principale è stata divisa in quattro sezioni principali: i comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra, nella parte centrale, è disponibile la finestra Descrizione e, infine, nella parte inferiore destra della schermata viene visualizzata la finestra Dettagli. Nella sezione Stato rapporto sono elencati i parametri principali di un rapporto (filtro usato, tipo di filtro, se il rapporto è il risultato di un confronto e così via).



4.7.2.1 Comandi del programma

La presente sezione contiene la descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Selezionare **File** per memorizzare lo stato attuale del sistema per un'analisi futura oppure aprire un rapporto precedentemente archiviato. Ai fini della pubblicazione, è consigliabile generare un rapporto **Adatto per l'invio**. In questo formato, nel rapporto vengono omesse informazioni sensibili (nome utente attuale, nome computer, nome dominio, privilegi utente attuale, variabili d'ambiente e così via).

NOTA: è possibile aprire i rapporti di ESET SysInspector precedentemente archiviati trascinandoli nella finestra principale.

Struttura

Consente di espandere o chiudere tutti i nodi e di esportare le sezioni selezionate sullo script di servizio.

Elenco

Contiene funzioni per uno spostamento più pratico all'interno del programma e varie altre funzioni, ad esempio la ricerca di informazioni su Internet.

Guida

Contiene informazioni sull'applicazione e sulle relative funzioni.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra principale al fine di semplificarne l'utilizzo. Nella modalità "Base" si ha accesso alle informazioni utilizzate per trovare soluzioni a problemi comuni del sistema. Nella modalità "Media" il programma visualizza i dettagli meno utilizzati, mentre nella modalità "Completa", ESET SysInspector mostra tutte le informazioni necessarie alla soluzione di problemi specifici.

Filtraggio elementi

Il filtraggio elementi viene utilizzato soprattutto per individuare file o voci di registro sospetti all'interno del sistema. Regolando il cursore, è possibile filtrare gli elementi in base al livello di rischio. Se il cursore si trova all'estrema sinistra (Livello di rischio 1) vengono visualizzati tutti gli elementi. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio attuale, visualizzando solo gli elementi che risultano più sospetti rispetto al livello visualizzato. Quando il cursore si trova all'estrema destra, il programma visualizza solo gli elementi dannosi conosciuti.

Tutti gli elementi contrassegnati con un livello di rischio compreso tra 6 e 9 rappresentano un rischio per la sicurezza. Se ESET SysInspector ha rilevato un elemento di questo tipo, si consiglia di eseguire il controllo del sistema con ESET Online Scanner, se non si utilizzano alcune delle soluzioni di protezione di ESET. ESET Online Scanner è un servizio gratuito.

NOTA: il Livello di rischio di un elemento può essere determinato rapidamente confrontandone il colore con quello del cursore Livello di rischio.

Cerca

L'opzione Cerca può essere utilizzata per individuare rapidamente un elemento specifico in base al nome o parte di esso. I risultati della richiesta di ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

Facendo clic sulla freccia indietro o avanti è possibile tornare alle informazioni precedentemente visualizzate nella finestra Descrizione. Utilizzare i tasti Cancella e Barra spaziatrice anziché fare clic avanti e indietro all'interno del programma.

Sezione stato

Visualizza il nodo corrente nella finestra di spostamento.

Importante: gli elementi evidenziati in rosso sono sconosciuti. Per tale motivo, il programma li segna come potenzialmente pericolosi. Se un elemento è segnalato in rosso, non implica automaticamente che sia possibile eliminare il file. Prima di procedere all'eliminazione, assicurarsi che i file siano effettivamente pericolosi o non necessari.

4.7.2.2 Spostarsi all'interno di ESET SysInspector

ESET SysInspector divide vari tipi di informazioni in numerose sezioni di base, dette nodi. Se disponibili, ulteriori dettagli saranno visualizzabili espandendo ciascun nodo nei relativi sottonodi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo o, in alternativa, selezionare + o − accanto al nome del nodo. Spostandosi nella struttura ad albero di nodi e sottonodi della finestra di spostamento, sono disponibili vari dettagli su ciascun nodo presente nella finestra Descrizione. Spostandosi tra gli elementi della finestra Descrizione, è possibile visualizzare ulteriori dettagli relativi a ciascun elemento nella finestra Dettagli.

Di seguito vengono riportate le descrizioni dei nodi principali presenti nella finestra di spostamento e le relative informazioni delle finestre Descrizione e Dettagli.

Processi in esecuzione

Questo nodo contiene informazioni sulle applicazioni e sui processi in esecuzione durante la generazione del rapporto. Nella finestra Descrizione sono disponibili dettagli aggiuntivi su ciascun processo, ad esempio le librerie dinamiche utilizzate dal processo e la loro posizione nel sistema, il nome del produttore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

NOTA: un sistema operativo è basato su diversi componenti kernel, in esecuzione 24 ore su 24, 7 giorni su 7, che

forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, tali processi sono visualizzati nello strumento ESET SysInspector con il percorso file preceduto da \??\. Quei simboli forniscono un'ottimizzazione per i processi in questione prima di avviarli e risultano sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e applicazioni che comunicano sulla rete utilizzando il protocollo selezionato nella finestra di spostamento (TCP o UDP), unitamente all'indirizzo remoto a cui è collegata l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

Voci importanti del Registro di sistema

Contiene un elenco delle voci di registro selezionate che sono spesso correlate a vari problemi del sistema, ad esempio quelle che indicano i programmi di avvio, oggetti browser helper (BHO) e così via.

Nella finestra Descrizione è possibile visualizzare i file correlati a voci di registro specifiche. Nella finestra Dettagli è possibile visualizzare maggiori informazioni.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi Windows. Nella finestra Dettagli è possibile controllare il modo in cui è impostato l'avvio del servizio insieme ai dettagli specifici del file.

Driver

Un elenco di driver installati nel sistema.

File critici

Nella finestra Descrizione è visualizzato il contenuto dei file critici relativi al sistema operativo Microsoft Windows.

Attività di pianificazione di sistema

Contiene un elenco delle attività avviate dall'Utilità di pianificazione di Windows a un orario/intervallo specificato.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e sul software, oltre a informazioni sulle variabili d'ambiente impostate, sui diritti utente e sui rapporti eventi di sistema.

Dettagli file

Un elenco di file di sistema importanti e di file presenti nella cartella Programmi. Per maggiori informazioni sui file in questione, fare riferimento alle finestre Descrizione e Dettagli.

Informazioni su

Informazioni sulla versione di ESET SysInspector ed elenco dei moduli del programma.

4.7.2.2.1 Tasti di scelta rapida

I tasti di scelta rapida che possono essere utilizzati con ESET SysInspector includono:

File

Ctrl+O	apre il rapporto esistente
Ctrl+S	salva i rapporti creati

Genera

Ctrl+G	genera uno snapshot di stato computer standard
Ctrl+H	genera uno snapshot di stato computer che potrebbe registrare anche informazioni sensibili

Filtraggio elementi

1, O	non a rischio, visualizzati gli elementi con livello di rischio 1-9

2	non a rischio, visualizzati gli elementi con livello di rischio 2-9
3	non a rischio, visualizzati gli elementi con livello di rischio 3-9
4, U	sconosciuto, visualizzati gli elementi con livello di rischio 4-9
5	sconosciuto, visualizzati gli elementi con livello di rischio 5-9
6	sconosciuto, visualizzati gli elementi con livello di rischio 6-9
7, B	a rischio, visualizzati gli elementi con livello di rischio 7-9
8	a rischio, visualizzati gli elementi con livello di rischio 8-9
9	a rischio, visualizzati gli elementi con livello di rischio 9
-	diminuisce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello uguale o più alto
Ctrl+O	modalità di filtraggio, solo livello uguale

Visualizza

Ctrl+5	visualizza per fornitore, tutti i fornitori
Ctrl+6	visualizza per fornitore, solo Microsoft
Ctrl+7	visualizza per fornitore, tutti gli altri fornitori
Ctrl+3	mostra tutti i dettagli
Ctrl+2	livello di dettaglio medio
Ctrl+1	visualizzazione di base
Cancella	indietro di un passaggio
Barra spaziatrice	avanti di un passaggio
Ctrl+W	espande la struttura
Ctrl+Q	comprime la struttura

Altri comandi

Ctrl+T	va alla posizione originale dell'elemento dopo averlo selezionato nei risultati di ricerca
Ctrl+P	visualizza informazioni di base su un elemento
Ctrl+A	visualizza informazioni complete su un elemento
Ctrl+C	copia la struttura dell'elemento corrente
Ctrl+X	copia gli elementi
Ctrl+B	trova su Internet le informazioni sui file selezionati
Ctrl+L	apre la cartella dove si trova il file selezionato
Ctrl+R	apre la voce corrispondente nell'editor del Registro di sistema
Ctrl+Z	copia un percorso di un file (se l'elemento è relativo a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	visualizza tutti gli elementi
Ctrl+Alt+2	visualizza solo gli elementi aggiunti, il rapporto mostrerà gli elementi presenti nel rapporto corrente
Ctrl+Alt+3	visualizza solo gli elementi rimossi, il rapporto mostrerà gli elementi presenti nel rapporto precedente
Ctrl+Alt+4	visualizza solo gli elementi sostituiti (compresi i file)
Ctrl+Alt+5	visualizza solo le differenze tra i rapporti
Ctrl+Alt+C	visualizza il confronto
Ctrl+Alt+N	visualizza il rapporto corrente
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza la guida
Alt+F4	chiude il programma
Alt+Maiusc+F4	chiude il programma senza chiedere
Ctrl+I	statistiche rapporto

4.7.2.3 Confronta

La funzione Confronta consente di mettere a confronto due rapporti esistenti. Il risultato di questa funzione è una serie di elementi non comuni ai due rapporti. È la soluzione adatta se si desidera rilevare le modifiche nel sistema ed è un utile strumento per individuare l'attività del codice dannoso.

Dopo l'avvio, l'applicazione crea un nuovo rapporto, visualizzato in una nuova finestra. Andare a **File** > **Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere aperti e visualizzati in un secondo momento. Per aprire un rapporto esistente, accedere a **File** > **Apri rapporto**. Nella finestra principale del programma, ESET SysInspector visualizza sempre un rapporto alla volta.

Il confronto tra due rapporti offre il vantaggio di visualizzare un rapporto attualmente attivo e uno salvato in un file. Per confrontare due rapporti, utilizzare l'opzione **File** > **Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Nel rapporto comparativo saranno visualizzate solo le differenze tra i due.

NOTA: se si mettono a confronto due file di rapporto, selezionando **File** > **Salva rapporto** e salvandoli in un file ZIP, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti verranno automaticamente messi a confronto.

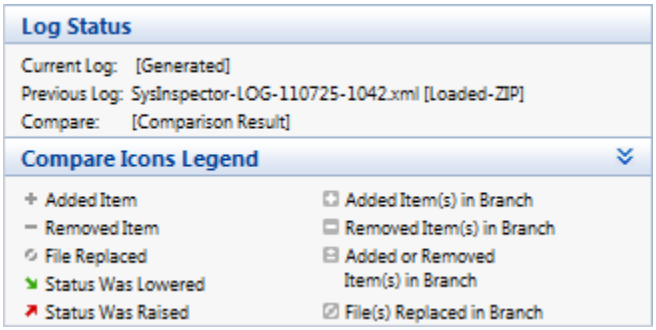
Accanto agli elementi visualizzati, ESET SysInspector mostra i simboli che identificano le differenze tra i rapporti confrontati.

Gli elementi contrassegnati con – si trovano solo nel rapporto attivo e non erano presenti nel rapporto comparativo aperto. Gli elementi contrassegnati con + erano presenti solo nel rapporto aperto e non sono presenti in quello attivo.

Descrizione di tutti i simboli che possono essere visualizzati accanto agli elementi:

- + nuovo valore, non presente nel rapporto precedente
- la sezione della struttura contiene nuovi valori
- – valore rimosso, presente solo nel rapporto precedente
- la sezione della struttura contiene i valori rimossi
- il valore/file è stato modificato
- la sezione della struttura contiene valori/file modificati
- il livello di rischio è diminuito/era più alto nel precedente rapporto
- il livello di rischio è aumentato/era più basso nel precedente rapporto

Nella sezione relativa alla descrizione visualizzata nell'angolo in basso a sinistra vengono descritti tutti i simboli e mostrati i nomi dei rapporti messi a confronto.



Qualsiasi rapporto comparativo può essere salvato in un file e aperto successivamente.

Esempio

Generare e salvare un rapporto, registrando le informazioni originali sul sistema, in un file denominato previous.xml. Dopo aver apportato le modifiche al sistema, aprire ESET SysInspector e attendere che venga generato un nuovo rapporto. Salvarlo in un file denominato *current.xml*.

Al fine di rilevare le modifiche tra i due rapporti, andare a **File** > **Confronta rapporti**. Il programma crea un rapporto comparativo che visualizza le differenze tra i due.

È possibile ottenere lo stesso risultato utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

4.7.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando con i seguenti parametri:

/gen	genera un rapporto direttamente dalla riga di comando senza eseguire l'interfaccia utente
/privacy	genera un rapporto escludendo informazioni sensibili
/zip	archivia il rapporto risultante direttamente sul disco in un file compresso
/silent	nasconde la barra di avanzamento della generazione del rapporto
/help, /?	visualizza informazioni sui parametri della riga di comando

Esempi

Per caricare un rapporto specifico direttamente nel browser, digitare: *SysInspector.exe "c:\clientlog.xml"*
Per generare un rapporto in un percorso corrente, digitare: *SysInspector.exe /gen*
Per generare un rapporto in una cartella specifica, digitare: *SysInspector.exe /gen="c:\folder\"*
Per generare un rapporto in un file/percorso specifico, digitare: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Per generare un rapporto escludendo le informazioni sensibili direttamente in un file compresso, digitare: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Per confrontare due rapporti, digitare: *SysInspector.exe "current.xml" "original.xml"*

NOTA: se il nome di un file/cartella contiene uno spazio vuoto, è necessario inserirlo tra virgolette.

4.7.4 Script di servizio

Lo script di servizio è uno strumento utile per i clienti che utilizzano ESET SysInspector in quanto consente di rimuovere facilmente gli oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto di ESET SysInspector o le parti selezionate. Al termine dell'esportazione, è possibile selezionare gli oggetti indesiderati da eliminare. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto agli utenti avanzati che hanno già acquisito esperienza nella diagnostica dei problemi del sistema. Le modifiche effettuate da persone non qualificate potrebbero causare danni al sistema operativo.

Esempio

Se si sospetta che il computer sia infettato da un virus non rilevato dal programma antivirus, attenersi alle seguenti istruzioni dettagliate:

- Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
- Selezionare il primo elemento della sezione a sinistra (nella struttura ad albero), premere Ctrl ed evidenziare l'ultimo elemento per selezionarli tutti.
- Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere l'opzione del menu contestuale **Esporta sezioni selezionate a script di servizio**.
- Gli oggetti selezionati verranno esportati in un nuovo rapporto.
- Questo è il passaggio più importante dell'intera procedura: aprire il nuovo rapporto e cambiare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Fare attenzione a non contrassegnare file/oggetti importanti del sistema operativo.
- Aprire ESET SysInspector, fare clic su **File** > **Esegui script di servizio** e immettere il percorso dello script.
- Fare clic su **OK** per eseguire lo script.

4.7.4.1 Generazione dello script di servizio

Per generare uno script, fare clic con il pulsante destro del mouse su qualsiasi voce della struttura del menu (nel riquadro a sinistra) nella finestra principale di ESET SysInspector. Selezionare l'opzione **Esporta tutte le sezioni a script di servizio** o l'opzione **Esporta sezioni selezionate a script di servizio** nel menu contestuale.

NOTA: non è possibile esportare lo script di servizio quando vengono confrontati due rapporti.

4.7.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script sono disponibili informazioni sulla versione del motore (ev), sulla versione dell'interfaccia utente (gv) e sulla versione del rapporto (lv). Questi dati possono essere utilizzati per tenere traccia delle possibili variazioni nel file XML che genera lo script e prevenire eventuali incoerenze durante l'esecuzione. Non modificare questa parte dello script.

La restante parte del file è suddivisa in sezioni in cui è possibile modificare gli elementi (indicare quelli che saranno elaborati dallo script). È possibile contrassegnare gli elementi da elaborare sostituendo il carattere "-" davanti a un elemento con il carattere "+". Le sezioni dello script sono separate tra loro mediante una riga vuota. A ogni sezione viene assegnato un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione nel sistema. Ogni processo è identificato mediante il proprio percorso UNC e, successivamente, dal rispettivo codice hash CRC16 tra asterischi (*).

Esempio:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Nell'esempio, è stato selezionato un processo, module32.exe (contrassegnato dal carattere "+"). Il processo terminerà all'esecuzione dello script.

02) Moduli caricati

In questa sezione sono contenuti i moduli di sistema attualmente in uso.

Esempio:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Nell'esempio, il modulo khbekhb.dll è stato contrassegnato con "+". All'esecuzione dello script, i processi che eseguono tale modulo specifico verranno riconosciuti e interrotti.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

All'esecuzione dello script, verrà individuato il proprietario del socket nelle connessioni TCP contrassegnate e il socket verrà interrotto, liberando le risorse del sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

All'esecuzione dello script, verrà isolato il proprietario del socket sugli endpoint UDP contrassegnati e il socket verrà interrotto.

05) Voci server DNS

Questa sezione contiene informazioni sulla configurazione del server DNS corrente.

Esempio:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

All'esecuzione dello script, le voci del server DNS contrassegnate verranno rimosse.

06) Voci importanti del Registro di sistema

Questa sezione contiene informazioni su importanti voci del Registro di sistema.

Esempio:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

All'esecuzione dello script, le voci contrassegnate verranno eliminate, ridotte a valori a 0 byte o ripristinate sui valori predefiniti. L'azione da eseguire su una particolare voce dipende dalla categoria della voce stessa e dal valore principale nel Registro di sistema specifico.

07) Servizi

In questa sezione sono riportati i servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup:
Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup:
Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

All'esecuzione dello script, i servizi contrassegnati e i relativi servizi dipendenti verranno interrotti e disinstallati.

08) Driver

In questa sezione sono riportati i driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando si esegue lo script, i driver selezionati verranno arrestati. Tenere presente che alcuni driver non possono essere arrestati.

09) File critici

Questa sezione contiene informazioni sui file critici per il sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Gli elementi selezionati saranno eliminati o ripristinati sui valori originali.

4.7.4.3 Esecuzione degli script di servizio

Contrassegnare tutti gli elementi desiderati, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, verrà visualizzato il seguente messaggio: **Eseguire lo script di servizio "% Scriptname%"?** Dopo aver confermato, verrà visualizzato un altro messaggio per segnalare che lo script di servizio che si sta cercando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Verrà visualizzata una finestra di dialogo per confermare la corretta esecuzione dello script.

Se lo script è stato eseguito solo parzialmente, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Visualizzare il rapporto degli errori?** Selezionare **Sì** per visualizzare un rapporto completo degli errori in cui sono indicate le operazioni non eseguite.

Se lo script non viene riconosciuto, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio selezionato non è firmato. L'esecuzione di script sconosciuti o non firmati potrebbe causare seri danni ai dati nel computer. Eseguire lo script e le azioni?** Ciò potrebbe essere causato da incoerenze all'interno dello script (intestazione danneggiata, titolo della sezione danneggiato, linea vuota tra le sezioni e così via). È possibile riaprire il file di script e correggere gli errori all'interno dello script o creare un nuovo script di servizio.

4.7.5 Domande frequenti

ESET SysInspector richiede privilegi di amministratore per l'esecuzione?

Anche se per eseguire ESET SysInspector non sono necessari privilegi di amministratore, alcune informazioni raccolte possono essere visualizzate solo da un account amministratore. Eseguendo il programma come utente standard o utente con restrizioni, si raccoglieranno meno informazioni sull'ambiente operativo in uso.

ESET SysInspector crea un file di rapporto?

ESET SysInspector può creare un file di rapporto relativo alla configurazione del computer in uso. Per salvarlo, selezionare **File** > **Salva rapporto** dal menu principale. I rapporti vengono salvati nel formato XML. Per impostazione predefinita, i file vengono salvati nella directory *%USERPROFILE%\Documenti*, con una convenzione di denominazione file "SysInpsector-%COMPUTERNAME%-AAMMGG-HHMM.XML". Se preferibile, è possibile modificare la posizione e il nome del file di rapporto prima di salvarlo.

Come si visualizza il file di rapporto di ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e selezionare **File** > **Apri rapporto** dal menu principale. È anche possibile trascinare i file di rapporto all'interno dell'applicazione ESET SysInspector. Se è necessario consultare frequentemente i file di rapporto di ESET SysInspector, è consigliabile creare un collegamento sul Desktop al file SYSINSPECTOR.EXE. Sarà quindi sufficiente trascinare i file di rapporto sopra di esso per poterli visualizzare. Per motivi di protezione, in Windows Vista/7 la funzione di trascinamento della selezione tra finestre con differenti autorizzazioni di protezione potrebbe non essere disponibile.

È disponibile una specifica per il formato del file di rapporto? E per quanto riguarda un SDK?

Attualmente non è disponibile né una specifica per il file di rapporto né un SDK, in quanto il programma è ancora in

fase di sviluppo. Dopo il rilascio del programma, potrebbero essere forniti sulla base dei commenti e delle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio di un determinato oggetto?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro e così via), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto e ne valutano quindi le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso). Nel riquadro di spostamento a sinistra, le sezioni sono colorate sulla base del livello di rischio più elevato di un oggetto al loro interno.

Un livello di rischio "6 - Sconosciuto (rosso)" significa che un oggetto è pericoloso?

Le valutazioni di ESET SysInspector non garantiscono che un oggetto sia dannoso. Questa affermazione dovrebbe essere eseguita da un esperto di sicurezza. ESET SysInspector è progettato per fornire una rapida valutazione agli esperti di sicurezza, in modo da informarli su quali oggetti del sistema potrebbero richiedere una loro ulteriore analisi in presenza di comportamento anomalo.

Perché ESET SysInspector si collega a Internet quando viene avviato?

Al pari di molte applicazioni, ESET SysInspector è provvisto di firma digitale, un certificato che garantisce la pubblicazione del software da parte di ESET e l'assenza di alterazione dello stesso. Al fine di verificare il certificato, il sistema operativo contatta un'autorità di certificazione per verificare l'identità dell'autore del software. Si tratta di una procedura comune eseguita su tutti i programmi con firma digitale eseguiti in Microsoft Windows.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth assicura un efficace rilevamento dei rootkit.

Se il sistema viene attaccato da codice dannoso che si comporta come un rootkit, l'utente può essere esposto al rischio di perdita o furto dei dati. In assenza di uno strumento speciale anti-rootkit, è quasi impossibile rilevarli.

Perché a volte i file contrassegnati come "Firmati da MS" hanno contemporaneamente un "Nome aziendale" differente?

Quando si cerca di identificare la firma digitale di un file eseguibile, ESET SysInspector verifica innanzitutto se nel file è incorporata una firma digitale. Se viene trovata una firma digitale, il file verrà convalidato utilizzando tali informazioni. Se la firma digitale non viene trovata, ESI inizia a ricercare il file CAT corrispondente (Catalogo di protezione - *%systemroot%\system32\catroot*) contenente informazioni sul file eseguibile elaborato. Nel caso in cui dovesse trovare il file CAT appropriato, nel processo di convalida del file eseguibile verrà applicata la firma digitale di tale file CAT.

Per tale motivo, a volte i file contrassegnati come "Firmati da MS" hanno contemporaneamente un "Nome aziendale" differente.

Esempio:

Windows 2000 include l'applicazione HyperTerminal nel percorso *C:\Programmi\Windows NT*. Il file eseguibile dell'applicazione principale non è firmato a livello digitale, ma ESET SysInspector lo contrassegna come file firmato da Microsoft. Ciò dipende da un riferimento in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* che punta a *C:\Programmi\Windows NT\hypertrm.exe* (il principale file eseguibile dell'applicazione HyperTerminal) e *sp4.cat* è firmato a livello digitale da Microsoft.

4.7.6 ESET SysInspector come componente di ESET File Security

Per aprire la sezione ESET SysInspector in ESET File Security, fare clic su **Strumenti** > **ESET SysInspector**. Il sistema di gestione nella finestra di ESET SysInspector è simile a quello dei rapporti di controllo del computer o delle attività pianificate. Tutte le operazioni con gli snapshot del sistema (crea, visualizza, confronta, rimuovi ed esporta) sono accessibili con pochi clic.

La finestra di ESET SysInspector contiene informazioni di base sugli snapshot creati, quali data e ora di creazione, breve commento, nome dell'utente che ha creato lo snapshot e stato dello snapshot.

Per eseguire il confronto, la creazione o l'eliminazione degli snapshot, utilizzare i pulsanti corrispondenti nella parte inferiore della finestra di ESET SysInspector. Tali opzioni sono disponibili anche dal menu contestuale. Per visualizzare lo snapshot di sistema selezionato, utilizzare l'opzione **Mostra** del menu contestuale. Per esportare lo snapshot selezionato in un file, fare clic con il pulsante destro del mouse, quindi selezionare **Esporta...**.

Di seguito viene fornita una descrizione dettagliata delle opzioni disponibili:

- **Confronta** - Consente di confrontare due rapporti esistenti. È idonea se si desidera rilevare le modifiche tra il rapporto attuale e uno precedente. Per utilizzare questa opzione, selezionare due snapshot da mettere a confronto.
- **Crea...** - Consente di creare un nuovo record. È prima necessario inserire un breve commento sul record. Per visualizzare lo stato di avanzamento della procedura di creazione dello snapshot (relativamente allo snapshot in corso di generazione), fare riferimento alla colonna **Stato**. Tutti gli snapshot completati sono contrassegnati dallo stato **Creato**.
- **Elimina/Elimina tutto** - Consente di rimuovere le voci dall'elenco.
- **Esporta...** - Consente di salvare la voce selezionata in un file XML (anche in una versione compressa).

4.8 ESET SysRescue

ESET SysRescue è un'utilità che consente di creare un disco di avvio contenente una delle soluzioni ESET Security: può essere ESET NOD32 Antivirus, ESET Smart Security o anche uno dei prodotti per server. Il vantaggio principale offerto da ESET SysRescue consiste nel fatto che la soluzione ESET Security viene eseguita indipendentemente dal sistema operativo che la ospita e, al tempo stesso, dispone dell'accesso diretto al disco e all'intero file system. Ciò consente di rimuovere infiltrazioni che non sarebbe stato possibile eliminare in una situazione ordinaria, ad esempio durante l'esecuzione del sistema operativo.

4.8.1 Requisiti minimi

ESET SysRescue è eseguibile su Microsoft Windows Preinstallation Environment (Windows PE) versione 2.x, basato su Windows Vista.

Windows PE è incluso nel pacchetto gratuito Windows Automated Installation Kit (Windows AIK) o Windows Assessment and Deployment Kit (Windows ADK) e pertanto deve essere installato prima di procedere alla creazione di ESET SysRescue (http://go.eset.eu/AIK) o (http://go.eset.eu/ADK). Il tipo di kit che deve essere installato sul sistema dipende dalla versione del sistema operativo in esecuzione. A seguito del supporto della versione a 32 bit di Windows PE, è necessario usare un pacchetto di installazione della soluzione ESET Security a 32 bit durante la creazione di ESET SysRescue sui sistemi a 64 bit. ESET SysRescue supporta Windows AIK 1.1 e versioni successive, oltre a Windows ADK.

NOTA: poiché Windows AIK è superiore a 1 GB e Windows ADK è 1,3 GB, per un download lineare è necessaria una connessione Internet ad alta velocità.

ESET SysRescue è disponibile nelle soluzioni ESET Security 4.0 e versioni successive.

ESET SysRescue supporta i seguenti sistemi operativi:

- Windows Server 2003 Service Pack 1 con KB926044
- Windows Server 2003 Service Pack 2
- Windows Server 2008
- Windows Server 2012

Windows AIK supporta:

- Windows Server 2003
- Windows Server 2008

Windows ADK supporta:

- Windows Server 2012

4.8.2 Come creare un CD di ripristino

Per avviare la procedura guidata di ESET SysRescue, fare clic su **Start** > **Programmi** > **ESET** > **ESET File Security** > **ESET SysRescue**.

La procedura guidata rileva innanzitutto la presenza di Windows AIK o Windows ADK e di un dispositivo adatto alla creazione di un supporto di avvio. Se Windows AIK o Windows ADK non è installato nel computer, se è danneggiato o installato in modo errato, la procedura guidata consentirà di installarlo o di immettere il percorso della cartella di Windows AIK (http://go.eset.eu/AIK) o Windows ADK (http://go.eset.eu/ADK).

NOTA: poiché Windows AIK è superiore a 1 GB e Windows ADK è 1,3 GB, per un download lineare è necessaria una connessione Internet ad alta velocità.

Al passaggio successivo, selezionare il supporto di destinazione in cui si desidera posizionare ESET SysRescue.

4.8.3 Selezione delle destinazioni

Oltre che su CD/DVD/USB, è possibile scegliere di salvare ESET SysRescue anche in un file ISO. Successivamente, sarà possibile masterizzare l'immagine ISO su CD/DVD o utilizzarla in altro modo (ad esempio in ambienti virtuali quali VMware o Virtualbox).

Se è stato selezionato il dispositivo USB come supporto di destinazione, è possibile che su alcuni computer non sia possibile eseguire l'avvio. Alcune versioni del BIOS possono riportare problemi di comunicazione con Boot manager (ad esempio, con Windows Vista) e durante l'avvio vengono visualizzati i seguenti messaggi di errore:

```
file : \boot\bcd
stato : 0xc000000e
informazioni : si è verificato un errore durante il tentativo di leggere i dati della configurazione di avvio
```

Nel caso si verificasse questo tipo di errore, si consiglia di selezionare un supporto CD anziché USB.

4.8.4 Impostazioni

Prima di avviare la creazione di ESET SysRescue, nell'ultimo passaggio della procedura di installazione guidata di ESET SysRescue vengono visualizzati i parametri di compilazione. Tali parametri possono essere modificati facendo clic sul pulsante **Cambia...**. Le opzioni disponibili includono:

- Cartelle
- ESET Antivirus
- Avanzate
- Protocollo Internet
- Dispositivo USB di avvio (quando è selezionato il dispositivo USB di destinazione)
- Masterizzazione (quando è selezionata l'unità CD/DVD di destinazione)

Il pulsante **Crea** rimane inattivo se non viene specificato alcun pacchetto di installazione MSI o se nel computer non viene installata alcuna soluzione ESET Security. Per selezionare un pacchetto di installazione, fare clic sul pulsante **Cambia** e andare alla scheda **ESET Antivirus**. Se non si inseriscono nome utente e password (**Cambia** > **ESET Antivirus**), il pulsante **Crea** non è disponibile.

4.8.4.1 Cartelle

La **Cartella temporanea** è una cartella di lavoro per i file richiesti per la compilazione di ESET SysRescue.

Cartella ISO è una cartella in cui viene salvato, al termine della compilazione, il file ISO risultante.

L'elenco presente in questa scheda riporta tutte le unità di rete locali e mappate insieme allo spazio disponibile residuo. Se alcune cartelle si trovano in un'unità che non dispone di spazio sufficiente, si consiglia di selezionare un'unità alternativa che dispone di maggiore spazio. In caso contrario, è possibile che la compilazione si interrompa in modo anomalo a causa della mancanza di spazio libero su disco.

Applicazioni esterne - Consente di specificare programmi aggiuntivi che saranno eseguiti o installati dopo il riavvio da un supporto ESET SysRescue.

Includi applicazioni esterne - Consente di aggiungere programmi esterni alla compilazione di ESET SysRescue.

Cartella selezionata - Cartella in cui si trovano i programmi da aggiungere al disco di ESET SysRescue.

4.8.4.2 ESET Antivirus

Per la creazione di ESET SysRescue CD, è possibile selezionare due origini di file ESET utilizzabili dal compilatore.

Cartella ESS/EAV - File già contenuti nella cartella da cui la soluzione ESET Security è stata installata nel computer.

File MSI - Vengono utilizzati i file contenuti nel programma di installazione di MSI.

È quindi possibile scegliere di aggiornare il percorso dei file (NUP). Normalmente è consigliabile scegliere l'opzione predefinita **Cartella ESS/EAV/File MSI**. In alcuni casi, è possibile scegliere una **Cartella di aggiornamento** personalizzata, ad esempio per utilizzare una versione precedente o più recente del database delle firme antivirali.

È possibile utilizzare una delle due origini seguenti di nome utente e password:

ESS/EAV installato - Il nome utente e la password saranno copiati dalla soluzione ESET Security attualmente installata.

Da utente - Verranno utilizzati il nome utente e la password immessi nelle caselle di testo corrispondenti.

NOTA: la soluzione ESET Security su ESET SysRescue CD viene aggiornata da Internet o dalla soluzione ESET Security installata nel computer sul quale è in esecuzione ESET SysRescue CD.

4.8.4.3 Impostazioni avanzate

La scheda **Avanzate** consente di ottimizzare ESET SysRescue CD rispetto alle dimensioni della memoria del computer. Selezionare **576 MB o più** per scrivere il contenuto del CD nella memoria operativa (RAM). Se si seleziona **meno di 576 MB**, durante l'esecuzione di WinPE sarà sempre possibile accedere al CD di ripristino.

Nella sezione **Driver esterni** è possibile immettere i driver per gli hardware specifici utilizzati dall'utente (in genere, la scheda di rete). Sebbene WinPE sia basato su Windows Vista SP1, che supporta una vasta gamma di hardware, talvolta l'hardware non viene riconosciuto. È quindi necessario aggiungere il driver manualmente. Esistono due modi per introdurre il driver nella compilazione di ESET SysRescue: manualmente (mediante il pulsante **Aggiungi**) e automaticamente (mediante il pulsante **Ricerca aut.**). In caso di inserimento manuale, è necessario selezionare il percorso del file .inf corrispondente (è inoltre necessario che in questa cartella sia presente anche il file *.sys applicabile). In caso di introduzione automatica, il driver viene rilevato automaticamente nel sistema operativo di un determinato computer. Si consiglia di utilizzare l'inserimento automatico unicamente se ESET SysRescue viene utilizzato su un computer che dispone della stessa scheda di rete utilizzata dal computer in cui è stato creato ESET SysRescue CD. Durante la creazione, il driver di ESET SysRescue viene introdotto nella compilazione in modo tale che l'utente non debba cercarlo in seguito.

4.8.4.4 Protocollo Internet

Questa sezione consente di configurare le impostazioni di rete di base e le connessioni predefinite di ESET SysRescue.

Selezionare **Indirizzo IP privato automatico** per ottenere l'indirizzo IP automaticamente dal server DHCP (Dynamic Host Configuration Protocol).

In alternativa, questa connessione di rete può utilizzare un indirizzo IP specificato a livello manuale, anche noto come indirizzo IP statico. Selezionare **Personalizzato** per configurare le impostazioni IP appropriate. Se si seleziona questa opzione, è necessario specificare un **Indirizzo IP** e, per le connessioni LAN e Internet ad alta velocità, una **Maschera subnet**. In **Server DNS preferito** e **Server DNS alternativo**, digitare gli indirizzi del server DNS primario e secondario.

4.8.4.5 Dispositivo USB di avvio

Se è stato selezionato il dispositivo USB come supporto di destinazione, è possibile selezionare uno dei supporti USB disponibili nella scheda **Dispositivo USB di avvio** (nel caso siano presenti più dispositivi USB).

Selezionare il **Dispositivo** di destinazione appropriato dove sarà installato ESET SysRescue.

Attenzione: durante la creazione di ESET SysRescue, il dispositivo USB selezionato verrà formattato. Tutti i dati sul dispositivo verranno cancellati.

Se si seleziona l'opzione **Formattazione rapida**, la formattazione rimuove tutti i file dalla partizione ma non esegue il controllo del disco alla ricerca di settori errati. Usare questa opzione se il dispositivo USB è stato precedentemente formattato e si è certi che non sia danneggiato.

4.8.4.6 Masterizza

Se il supporto di destinazione selezionato è CD/DVD, è possibile specificare parametri aggiuntivi di masterizzazione nella scheda **Masterizza**.

Elimina file ISO - Selezionare questa opzione per eliminare il file ISO temporaneo dopo la creazione di ESET SysRescue CD.

Eliminazione attivata - Consente di selezionare le opzioni per l'eliminazione rapida e completa.

Dispositivo di masterizzazione - Selezionare l'unità da utilizzare per la masterizzazione.

Attenzione: questa è l'opzione predefinita. Se viene utilizzato un CD/DVD riscrivibile, tutti i dati in esso contenuti verranno eliminati.

La sezione Supporto contiene informazioni sul supporto nel dispositivo CD/DVD in uso.

Velocità di masterizzazione - Selezionare la velocità desiderata dal menu a discesa. Quando si seleziona la velocità di masterizzazione è necessario tener conto delle capacità del dispositivo di masterizzazione e del tipo di CD/DVD in uso.

4.8.5 Utilizzo di ESET SysRescue

Affinché il CD/DVD/USB di ripristino funzioni in maniera ottimale, è necessario avviare il computer dal supporto ESET SysRescue. È possibile modificare la priorità di avvio nel BIOS. In alternativa, è possibile utilizzare il menu di avvio durante l'inizializzazione del computer. In genere si utilizzano i tasti F9 o F12 a seconda della versione della scheda madre/BIOS in uso.

Dopo l'avvio dal supporto di avvio, la soluzione ESET Security viene inizializzata. Poiché ESET SysRescue viene utilizzato solo in situazioni specifiche, l'utilizzo di alcuni moduli di protezione e funzioni del programma disponibili nella versione standard della soluzione ESET Security non è richiesto. L'elenco di tali funzioni e moduli si limita alle operazioni di **Controllo computer**, **Aggiorna** e alcune sezioni in **Configurazione** La funzionalità più importante di ESET SysRescue è la capacità di aggiornare il database delle firme antivirali. Prima di avviare un controllo del computer, è pertanto consigliabile eseguire un aggiornamento del programma.

4.8.5.1 Utilizzo di ESET SysRescue

Si supponga che i computer nella rete siano stati infettati da un virus che modifica i file eseguibili (EXE). La soluzione ESET Security è in grado di pulire tutti i file infetti ad eccezione di *explorer.exe*, che non può essere pulito neanche in modalità sicura. Ciò dipende dal fatto che anche *explorer.exe*, in qualità di uno dei processi Windows essenziali, viene lanciato in modalità sicura. La soluzione ESET Security non riuscirebbe ad eseguire alcuna azione sul file, che rimarrebbe quindi infettato.

In questo tipo di scenario, è possibile usare ESET SysRescue per risolvere il problema. ESET SysRescue non richiede l'utilizzo di alcun componente del sistema operativo che lo ospita ed è pertanto in grado di elaborare (pulire, eliminare) qualsiasi file sul disco.

4.9 Interfaccia utente

Le opzioni di configurazione dell'interfaccia utente in ESET File Security consentono di modificare l'ambiente di lavoro per adattarlo alle esigenze specifiche dell'utente. Tali opzioni di configurazione sono disponibili nella sottostruttura **Interfaccia utente** della struttura Configurazione avanzata di ESET File Security.

Nella sezione **Elementi dell'interfaccia utente**, l'opzione **Modalità avanzata** consente all'utente di attivare/disattivare la modalità avanzata. Nella modalità avanzata sono disponibili impostazioni più dettagliate e controlli aggiuntivi per ESET File Security.

L'opzione **Interfaccia grafica utente** deve essere disattivata qualora gli elementi grafici rallentino le prestazioni del computer o causino altri problemi. Potrebbe inoltre essere necessario disattivare l'interfaccia grafica per gli utenti con problemi visivi in quanto potrebbe creare conflitto con determinate applicazioni utilizzate per leggere il testo visualizzato sullo schermo.

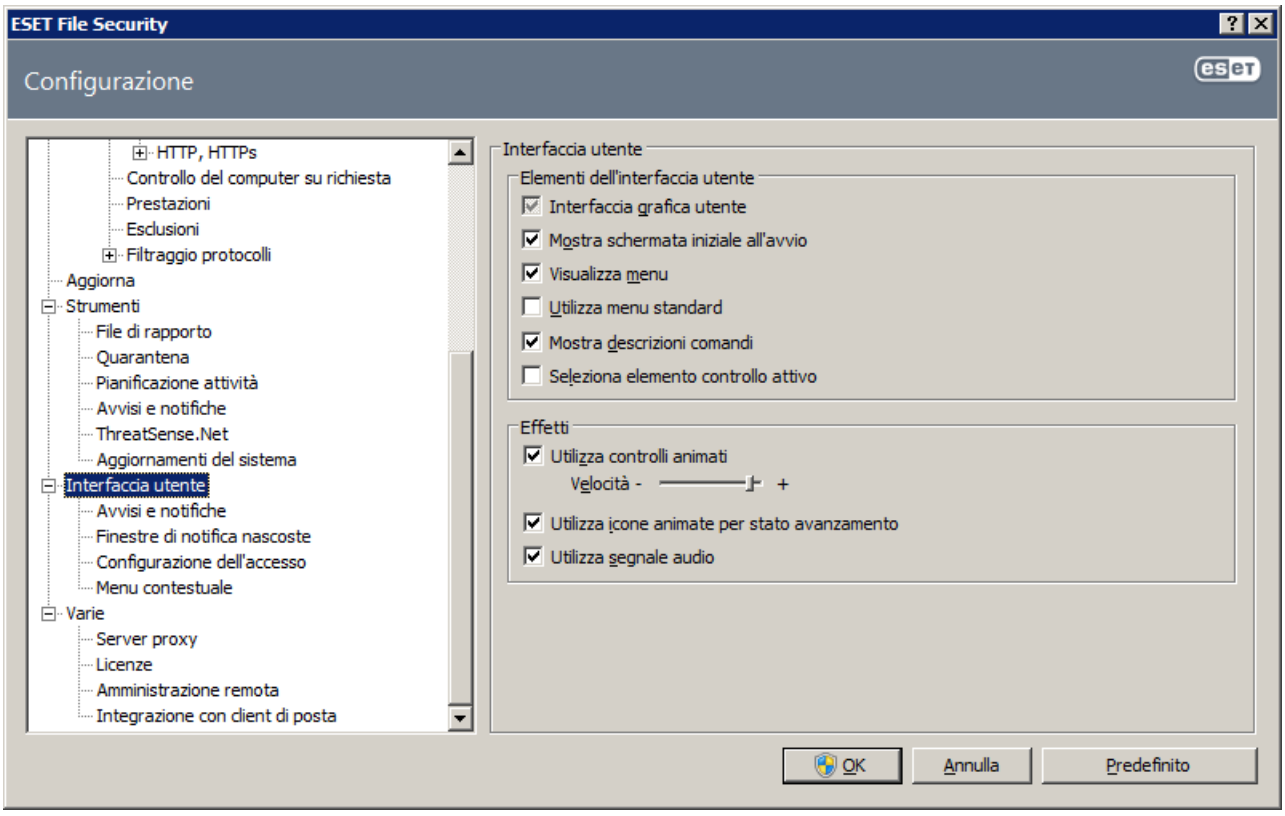
Per disattivare la schermata iniziale di ESET File Security, deselezionare l'opzione **Mostra schermata iniziale all'avvio**.

Nella parte superiore della finestra principale del programma di ESET File Security è disponibile un menu standard che può essere attivato o disattivato in base all'opzione **Utilizza menu standard**.

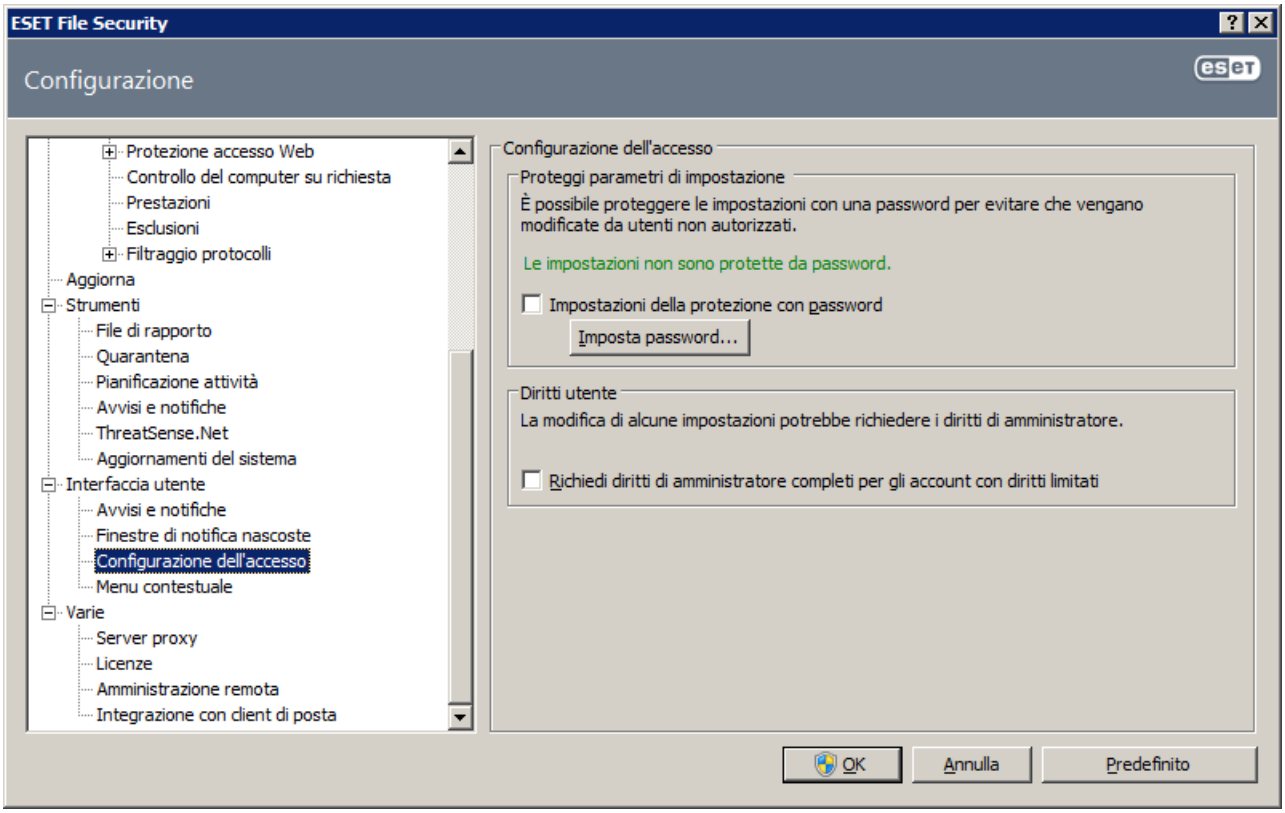
Se l'opzione **Mostra descrizioni comandi** è attivata, verrà visualizzata una breve descrizione quando si passa con il cursore sulle singole opzioni. Scegliendo l'opzione **Seleziona elemento controllo attivo**, verrà evidenziato l'elemento presente al momento nell'area attiva del cursore del mouse. Per attivare l'elemento evidenziato, fare clic su di esso.

Per aumentare o ridurre la velocità degli effetti animati, selezionare l'opzione **Utilizza controlli animati** e spostare il cursore di **Velocità** a destra o sinistra.

Per attivare l'utilizzo di icone animate per visualizzare lo stato di avanzamento di varie operazioni, selezionare l'opzione **Utilizza icone animate per stato avanzamento**. Se si desidera che il programma emetta un suono di allarme nel caso si verifichi un evento importante, selezionare l'opzione **Utilizza segnale audio**.



Le funzioni dell'**Interfaccia utente** includono anche l'opzione di proteggere con password i parametri di configurazione di ESET File Security. L'opzione è disponibile nel sottomenu **Impostazione protezione** nell' **Interfaccia utente**. Per garantire la massima sicurezza del sistema è fondamentale che il programma sia configurato correttamente. Modifiche non autorizzate possono causare la perdita di dati importanti. Per impostare una password per proteggere i parametri di impostazione, fare clic su **Imposta password...**.



4.9.1 Avvisi e notifiche

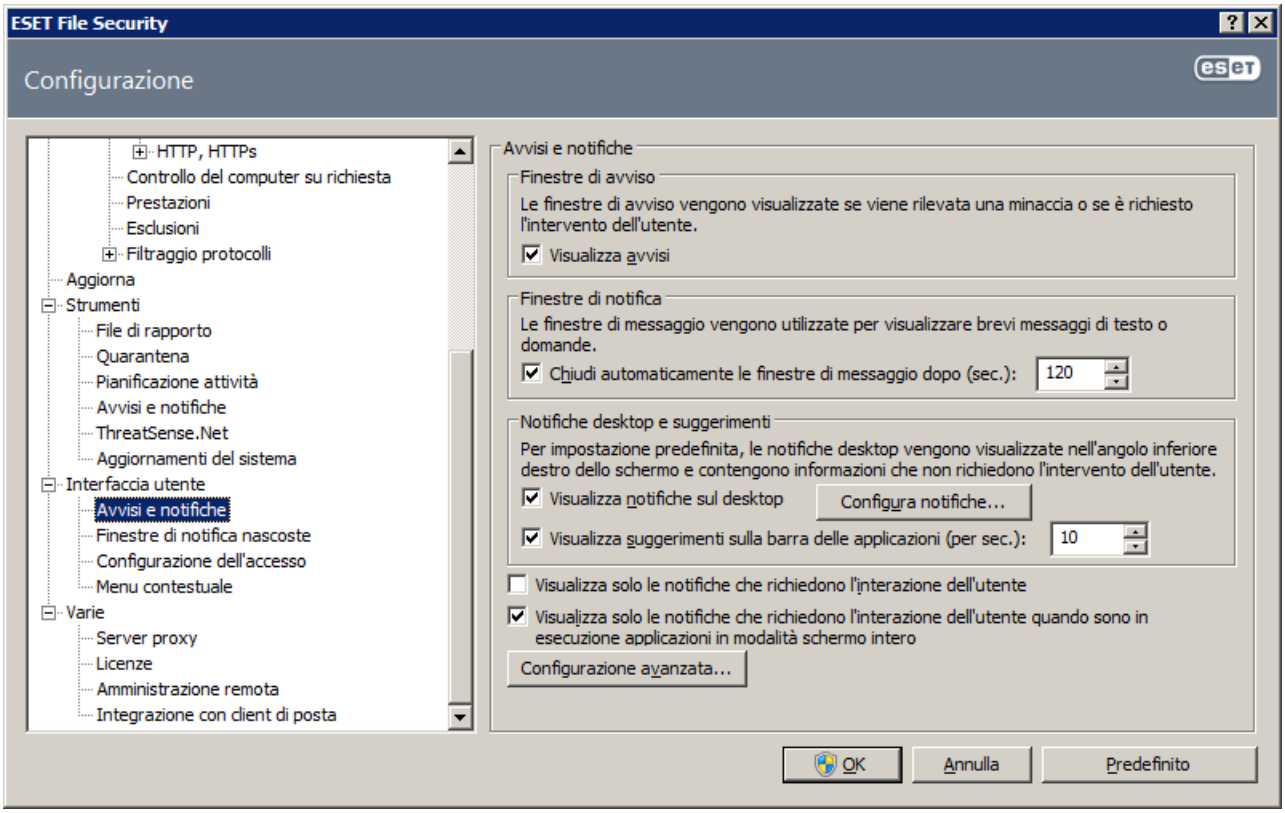
La sezione **Configurazione di avvisi e notifiche** nell'**Interfaccia utente** consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema in ESET File Security.

La prima voce da considerare è **Visualizza avvisi**. Se questa opzione viene disattivata, tutte le finestre di avviso vengono annullate. Per tale motivo, è consigliabile disattivarla solo in situazioni specifiche. Nella maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).

Per chiudere automaticamente le finestre popup dopo un determinato periodo di tempo, selezionare l'opzione **Chiudi automaticamente le finestre di messaggio dopo (sec.)**. Se non vengono chiuse manualmente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

Le notifiche visualizzate sul desktop e i suggerimenti sono solo a titolo informativo e non consentono o richiedono l'interazione da parte dell'utente. Vengono visualizzati nell'area di notifica posta nell'angolo in basso a destra della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare l'opzione **Visualizza notifiche sul desktop**. Per modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra, fare clic sul pulsante **Configura notifiche...**.

Per visualizzare in anteprima il funzionamento delle notifiche, fare clic sul pulsante **Anteprima**. Per configurare la durata di visualizzazione dei suggerimenti, vedere l'opzione **Visualizza suggerimenti sulla barra delle applicazioni (per sec.)**.



Fare clic su **Configurazione avanzata...** per immettere opzioni di configurazione aggiuntive degli **Avvisi e notifiche** che includono **Visualizza solo le notifiche che richiedono l'interazione dell'utente**. Questa opzione consente di attivare/disattivare la visualizzazione degli avvisi e delle notifiche che non richiedono interazione da parte dell'utente. Selezionare **Visualizza solo le notifiche che richiedono l'interazione dell'utente quando sono in esecuzione applicazioni in modalità a schermo intero** per non visualizzare tutte le notifiche non interattive. Nel menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** è possibile selezionare il livello iniziale di gravità degli avvisi e delle notifiche da visualizzare.

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multi-utente. Il campo **In sistemi multiutente**, **visualizza le notifiche sullo schermo di questo utente**: consente di definire gli utenti che riceveranno notifiche importanti da ESET File Security. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

4.9.2 Disattiva l'interfaccia utente su Terminal Server

In questo capitolo viene illustrato come disattivare l'interfaccia utente di ESET File Security in esecuzione su Windows Terminal Server per le sessioni utente.

In genere l'interfaccia utente di ESET File Security viene avviata ogni volta che un utente remoto accede al server e crea una sessione terminal. Ciò non è di norma auspicabile sui Terminal Server. Se si desidera disattivare l'interfaccia utente per le sessioni terminal, attenersi ai seguenti passaggi:

1. Eseguire *regedit.exe*
2. Accedere a *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Fare clic con il pulsante destro del mouse sul valore *egui* e selezionare *Modifica.*.
4. Aggiungere un'opzione `/terminal` alla fine di una stringa esistente

Di seguito viene riportato un esempio di come i dati Valore di *egui* dovrebbero apparire:

```
"C:\Programmi\ESET\ESET File Security\egui.exe" /hide /waitservice /terminal
```

Se si desidera ripristinare questa impostazione e consentire l'avvio automatico dell'interfaccia utente di ESET File Security, rimuovere l'opzione `/terminal` . Per accedere al valore di registro *egui*, ripetere i passaggi da 1 a 3.

4.10 eShell

eShell (abbreviazione di ESET Shell) è un'interfaccia della riga di comando per ESET File Security. Rappresenta un'alternativa all'interfaccia grafica utente (GUI). eShell offre tutte le funzionalità e le opzioni generalmente offerte dalla GUI. eShell consente di configurare e amministrare l'intero programma senza utilizzare la GUI.

In aggiunta a tutte le funzionalità disponibili nella GUI, offre anche l'opzione di utilizzo dell'automazione mediante l'esecuzione di script per poter configurare, modificare la configurazione o eseguire un'azione. eShell può inoltre risultare utile per gli utenti che preferiscono utilizzare la riga di comando rispetto alla GUI.

In questa sezione viene illustrato come spostarsi all'interno di eShell e le rispettive modalità di utilizzo, oltre a tutti i comandi con la descrizione di quale particolare comando viene utilizzato e l'azione che esegue.

eShell può essere eseguito in due modalità:

- Modalità interattiva - Risulta utile quando si desidera utilizzare eShell (non eseguire semplicemente un singolo comando) per attività quali la modifica della configurazione, la visualizzazione dei rapporti e così via. La modalità interattiva può essere utilizzata anche se ancora non si è familiarizzato con tutti i comandi. La modalità interattiva consente lo spostamento all'interno di eShell. Vengono inoltre visualizzati i comandi disponibili che è possibile utilizzare all'interno di un particolare contesto.
- Singolo comando/modalità batch - Questa modalità può essere utilizzata se è necessario eseguire solo un comando senza accedere alla modalità interattiva di eShell. Questa operazione può essere eseguita dal prompt dei comandi di Windows digitando `eshell` con i comandi appropriati. Ad esempio:

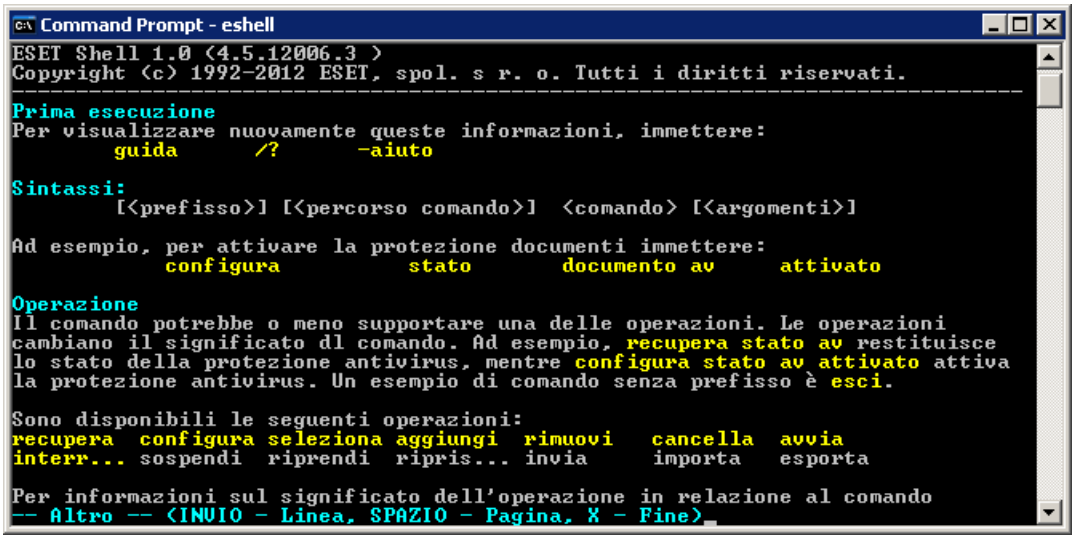
```
eshell set av document status enabled
```

NOTA: per eseguire i comandi di eShell dal prompt dei comandi di Windows o per eseguire i file batch, è necessario aver prima attivato questo funzione (è necessario che il comando `set general access batch always` sia eseguito nella modalità interattiva). Per ulteriori informazioni sul comando set batch, fare clic qui.

Per accedere alla modalità interattiva in eShell, è possibile utilizzare uno dei due metodi seguenti:

- Tramite il menu Start di Windows: **Start** > **Programmi** > **ESET** > **ESET File Security** > **ESET shell**
- Dal prompt dei comandi di Windows digitando `eshell` e premendo il tasto INVIO.

Quando si esegue eShell nella modalità interattiva per la prima volta, viene visualizzata la schermata della prima esecuzione.


Command Prompt - eshell
ESET Shell 1.0 (4.5.12006.3)
Copyright (c) 1992-2012 ESET, spol. s r. o. Tutti i diritti riservati.
Prima esecuzione
Per visualizzare nuovamente queste informazioni, immettere:
guida /? -aiuto
Sintassi:
[<prefisso>] [<percorso comando>] <comando> [<argomenti>]
Ad esempio, per attivare la protezione documenti immettere:
configura stato documento av attivato
Operazione
Il comando potrebbe o meno supportare una delle operazioni. Le operazioni
cambiano il significato dl comando. Ad esempio, recupera stato av restituisce
lo stato della protezione antivirus, mentre configura stato av attivato attiva
la protezione antivirus. Un esempio di comando senza prefisso è esci.
Sono disponibili le seguenti operazioni:
recupera configura seleziona aggiungi rimuovi cancella avvia
interr... sospendi riprendi ripris... invia importa esporta
Per informazioni sul significato dell'operazione in relazione al comando
-- Altro -- (INVIO - Linea, SPAZIO - Pagina, X - Fine)

In questa schermata vengono visualizzati esempi di base su come utilizzare eShell con Sintassi, Prefisso, Percorso comando, Forme abbreviate, Alias e così via. Si tratta essenzialmente di una guida rapida all'utilizzo di eShell.

NOTA: se si desidera visualizzare in futuro la schermata della prima esecuzione, digitare il comando `guide` .

NOTA: i comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

4.10.1 Utilizzo

Sintassi
Per un corretto funzionamento, i comandi devono essere formattati nella sintassi corretta e devono essere composti da un prefisso, un contesto, argomenti, opzioni e così via. Di seguito viene riportata la sintassi generale utilizzata all'interno di eShell:

[<prefisso>] [<percorso comando>] <comando> [<argomenti>]

Esempio (verrà attivata la protezione del documento):
`SET AV DOCUMENT STATUS ENABLED`

`SET` - un prefisso
`AV DOCUMENT` - percorso a un particolare comando, un contesto al quale appartiene tale comando
`STATUS` - il comando stesso
`ENABLED` - un argomento per il comando

L'utilizzo di `HELP` o `?` con un comando consente di visualizzare la sintassi di tale comando specifico. Ad esempio, `CLEANLEVEL HELP` consente di visualizzare la sintassi per il comando `CLEANLEVEL` :

SINTASSI:
```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

Si noti che `[get]` viene racchiuso tra parentesi quadre. Indica che il prefisso `get` è il prefisso predefinito per il comando `cleanlevel` . Ciò significa che quando si esegue il comando `cleanlevel` senza specificare un prefisso, verrà utilizzato in realtà il prefisso predefinito (in questo caso `get cleanlevel`). L'utilizzo di comandi senza un prefisso consente di ridurre i tempi di digitazione. In genere `get` rappresenta il prefisso predefinito per la maggior parte dei comandi, ma è necessario accertarsi quale sia il prefisso predefinito per un determinato comando e che sia esattamente quello che si desidera eseguire.

NOTA: i comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

Prefisso/operazione
Un prefisso rappresenta un'operazione. Il prefisso `GET` fornisce informazioni sulle modalità di configurazione di una determinata funzionalità di ESET File Security o consente di visualizzare lo stato, ad esempio `GET AV STATUS` mostra lo stato di protezione corrente. Il prefisso `SET` consente di configurare la funzionalità o di modificarne lo stato (`SET AV STATUS ENABLED` attiva la protezione).

Questi sono i prefissi che eShell consente di utilizzare. Un comando può o meno supportare uno dei seguenti prefissi

`GET` - ripristina impostazione/stato corrente
`SET` - configura valore/stato
`SELECT` - seleziona una voce
`ADD` - aggiunge una voce
`REMOVE` - rimuove una voce
`CLEAR` - rimuove tutti gli elementi/file
`START` - avvia un'azione
`STOP` - interrompe un'azione
`PAUSE` - sospende un'azione
`RESUME` - riprende un'azione
`RESTORE` - ripristina impostazioni predefinite/oggetto/file
`SEND` - invia un oggetto/file
`IMPORT` - importa da un file
`EXPORT` - esporta in un file

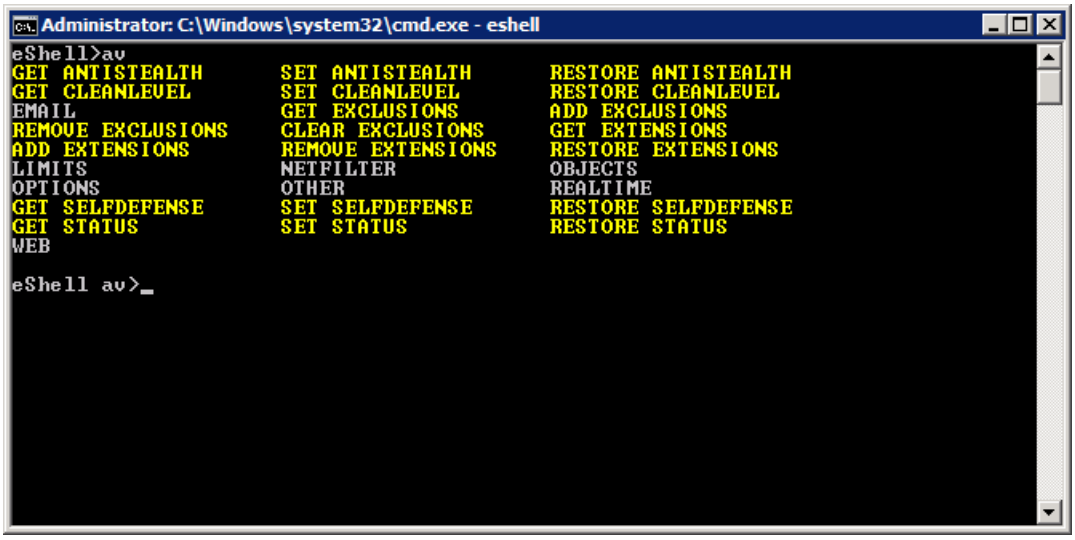
I prefissi quali `GET` e `SET` vengono utilizzati con numerosi comandi ma alcuni di essi (ad esempio `EXIT`) non utilizzano un prefisso.

Percorso del comando/contesto
I comandi sono posizionati in contesti che formano una struttura ad albero. Il livello superiore dell'albero è la radice. Quando si esegue eShell, si è al livello radice:

```
eShell>
```

È possibile eseguire un comando da tale posizione oppure immettere il nome del contesto per spostarsi all'interno

della struttura ad albero. Ad esempio, quando si accede al contesto `TOOLS`, verranno elencati tutti i comandi e sottocontesti disponibili da questa posizione.



Le voci in giallo sono i comandi che è possibile eseguire, mentre quelle in grigio sono i sottocontesti ai quali è possibile accedere. Un sottocontesto contiene ulteriori comandi.

Se è necessario ritornare a un livello superiore, utilizzare `..` (due punti). Ad esempio, se ci si trova nel contesto

```
eShell av options>
```

digitare `..` per passare a un livello superiore, ovvero a

```
eShell av>
```

Se si desidera ritornare alla radice da `eShell av options>` (che si trova a due livelli inferiori dalla radice), è sufficiente digitare `..  ..` (due punti e due punti separati da spazio). In questo modo, si passa a due livelli superiori che, in questo caso, corrispondono alla radice. Tale accorgimento può essere utilizzato indipendentemente dal livello all'interno della struttura dei contesti in cui ci si trova. Utilizzare il numero appropriato di `..` per passare al livello desiderato.

Il percorso è relativo al contesto corrente. Se il comando è contenuto nel contesto corrente, non immettere un percorso. Ad esempio, per eseguire `GET AV STATUS` immettere:

`GET AV STATUS` - se ci si trova nel contesto radice (sulla riga di comando è visualizzato `eShell>`)
`GET STATUS` - se ci si trova nel contesto `AV` (sulla riga di comando è visualizzato `eShell av>`)
`.. GET STATUS` - se ci si trova nel contesto `AV OPTIONS` (sulla riga di comando è visualizzato `eShell av options>`)

Argomento

Un argomento è un'azione che viene eseguita per un particolare comando. Ad esempio, il comando `CLEANLEVEL` può essere utilizzato con i seguenti argomenti:

`none` - Non pulire
`normal` - Pulitura standard
`strict` - Massima pulitura

Un altro esempio sono gli argomenti `ENABLED` o `DISABLED`che vengono utilizzati per attivare o disattivare una determinata funzionalità.

Forma abbreviata/comandi abbreviati

eShell consente di abbreviare i contesti, i comandi e gli argomenti (a condizione che l'argomento sia un'opzione oppure un'opzione alternativa). Non è possibile abbreviare un prefisso o un argomento che sia un valore concreto, ad esempio un numero, un nome o un percorso.

Esempi della forma breve:

```
set status enabled  => set stat en
add av exclusions C:\path\file.ext => add av exc C:\path\file.ext
```

Nel caso in cui due comandi o contesti inizino con la stessa lettera, ad esempio ABOUT e AV e si immette A come comando abbreviato, eShell non sarà in grado di scegliere quale comando dei due l'utente desidera eseguire. Verrà quindi visualizzato un messaggio di errore e verranno visualizzati i comandi che iniziano con la lettera "A" tra i quali scegliere:

```
eShell>a
Il seguente comando non è univoco: a

I seguenti comandi sono disponibili in questo contesto:
 ABOUT - Mostra informazioni sul programma
 AV - Modifiche sul contesto av
```

Aggiungendo una o più lettere (ad esempio AB anziché semplicemente A) eShell esegue il comando ABOUT poiché in questo caso risulta univoco.

NOTA: se si desidera essere certi che un comando venga eseguito come desiderato, si consiglia di non abbreviare i comandi, gli argomenti e così via e di utilizzare la forma completa. In questo modo, verrà eseguito esattamente come desiderato e si eviteranno errori indesiderati. Ciò è particolarmente utile nel caso dei file batch/script.

Alias

Un alias è un nome alternativo che può essere utilizzato per eseguire un comando, a condizione che al comando sia assegnato un alias. Sono disponibili alcuni alias predefiniti:

```
 (global) help - ?
(global) close - esci
(global) quit - esci
(global) bye - esci
warnlog - eventi rapporto strumenti
virlog - rilevamenti rapporto strumenti
```

"(global)" indica che il comando può essere utilizzato ovunque, indipendentemente dal contesto corrente. A un comando possono essere assegnati più alias. Ad esempio al comando EXIT è assegnato l'alias CLOSE, QUIT e BYE. Per uscire da eShell, è possibile utilizzare il comando EXIT oppure uno qualsiasi dei rispettivi alias. L'alias VIRLOG è per il comando DETECTIONS posizionato nel contesto TOOLS LOG. In questo modo, il comando Detections è disponibile dal contesto ROOT, facilitando l'accesso. (Non è infatti necessario accedere a TOOLS, quindi al contesto LOG ed eseguirlo direttamente da ROOT).

eShell consente di definire alias personali.

Comandi protetti

Alcuni comandi sono protetti e possono essere eseguiti solo dopo aver immesso una password.

Guide

Quando si esegue il comando GUIDE, verrà visualizzata una schermata "della prima esecuzione" in cui viene illustrato come utilizzare eShell. Questo comando è disponibile nel contesto ROOT (eShell>).

Help

Quando il comando HELP viene utilizzato da solo, verranno visualizzati tutti i comandi disponibili con i prefissi e i sottocontesti all'interno del contesto corrente. Viene inoltre fornita una breve descrizione di ciascun comando/sottocontesto. Quando si utilizza HELP come un argomento con un particolare comando, ad esempio CLEANLEVEL HELP, verranno fornite informazioni su tale comando. Verranno visualizzati SINTASSI, OPERAZIONI, ARGOMENTI e ALIAS per il comando, con una breve descrizione su ciascuno di essi.

Cronologia dei comandi

eShell conserva la cronologia dei comandi eseguiti in precedenza. Ciò è applicabile solo alla sessione eShell interattiva corrente. Quando si esce da eShell, la cronologia dei comandi non sarà più disponibile. Utilizzare i tasti freccia Su e Giù sulla tastiera per spostarsi all'interno della cronologia. Dopo aver trovato il comando desiderato, è possibile eseguirlo nuovamente o modificarlo senza doverlo digitare nuovamente dall'inizio.

CLS/Cancella schermata

Il comando CLS può essere utilizzato per cancellare la schermata. Funziona allo stesso modo del prompt dei comandi di Windows o delle interfacce della riga di comando simili.

EXIT / CLOSE / QUIT / BYE

Per chiudere o uscire da eShell, è possibile utilizzare uno di questi comandi (EXIT, CLOSE, QUIT o BYE).

4.10.2 Comandi

In questa sezione sono elencati tutti i comandi eShell disponibili con la relativa descrizione.

NOTA: i comandi non fanno distinzione tra lettera maiuscola e minuscola per poter essere eseguiti.

Comandi contenuti all'interno del contesto **ROOT**:

ABOUT

Mostra informazioni sul programma. Viene visualizzato il nome del prodotto installato, il numero di versione, i componenti installati, compreso il numero di versione di ciascun componente, e le informazioni di base sul server e il sistema operativo sul quale è in esecuzione ESET File Security.

PERCORSO CONTESTUALE:

`radice`

BATCH

Avvia la modalità batch eShell. Risulta molto utile quando si eseguono file batch/script. Si consiglia di utilizzare questo comando con i file batch. Inserire `START BATCH` come primo comando nel file batch o nello script per attivare la modalità batch. Quando si attiva questa funzione, non viene richiesta l'immissione di alcun comando interattivo, ad esempio l'inserimento di una password, e gli argomenti mancanti vengono sostituiti con quelli predefiniti. In questo modo si assicura che il file batch non verrà interrotto improvvisamente poiché eShell si aspetta che l'utente esegua una determinata azione. Il file batch dovrebbe quindi essere eseguito senza interruzione, a meno che non sia presente un errore o i comandi all'interno del file batch non siano errati.

PERCORSO CONTESTUALE:

`radice`

SINTASSI:

`[start] batch`

OPERAZIONI:

`start` - Avvia eShell nella modalità batch.

PERCORSO CONTESTUALE:

`radice`

ESEMPI:

`start batch` - Avvia la modalità batch di eShell

GUIDE

Mostra la schermata della prima esecuzione.

PERCORSO CONTESTUALE:

`radice`

PASSWORD

In genere, per motivi di sicurezza, per eseguire comandi protetti con password, all'utente viene chiesto di immettere una password. Ciò è applicabile a comandi che disattivano la protezione antivirus o che potrebbero influenzare la funzionalità di ESET File Security. A ogni esecuzione di tale comando, all'utente verrà chiesto di inserire la password. Per evitare di doverla inserire ogni volta, l'utente può definire la password, che verrà ricordata da eShell e utilizzata automaticamente a ogni esecuzione di un comando protetto con password. Ciò significa che non sarà necessario inserire ogni volta la password.

NOTA: la password impostata è valida solo per la sessione eShell interattiva corrente. Quando si esce da eShell, la password impostata non sarà più valida. Al successivo avvio di eShell, sarà necessario definirla nuovamente.

L'impostazione della password risulta inoltre molto utile anche quando si eseguono file batch/script. Di seguito viene riportato un esempio di file batch:

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

Il precedente comando concatenato avvia una modalità batch, definisce una password che verrà utilizzata e disattiva la protezione.

PERCORSO CONTESTUALE:

`radice`

SINTASSI:

```
[get] | restore password

set password [plain <password>]
```

OPERAZIONI:

`get` - Mostra password

`set` - Imposta o cancella la password

`restore` - Cancella la password

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

ESEMPI:

`set password plain <yourpassword>` - Imposta una password che verrà utilizzata per i comandi protetti con password

`restore password` - Cancella la password

ESEMPI:

`get password` - Utilizzare questo comando per visualizzare se la password è configurata o meno (verranno visualizzati solo asterischi "*" e non la password stessa). Se non sono visibili asterischi, significa che la password non è impostata

`set password plain <yourpassword>` - Utilizzare questo comando per impostare una password definita

`restore password` - Questo comando cancella la password definita

STATUS

Fornisce informazioni relative allo stato di protezione corrente di ESET File Security (simile all'interfaccia utente).

PERCORSO CONTESTUALE:

`radice`

SINTASSI:

```
[get] | restore status

set status disabled | enabled
```

OPERAZIONI:

`get` - Mostra lo stato della protezione antivirus

`set` - Disattiva/attiva la protezione antivirus

`restore` - Ripristina le impostazioni predefinite

ARGOMENTI:

`disabled` - Disattiva la protezione antivirus

`enabled` - Attiva la protezione antivirus

ESEMPI:

`get status` - Mostra lo stato di protezione corrente

`set status disabled` - Disattiva la protezione

`restore status` - Ripristina l'impostazione predefinita della protezione (Attivata)

VIRLOG

Alias del comando `DETECTIONS` . Risulta utile per visualizzare le informazioni sulle infiltrazioni rilevate.

WARNLOG

Alias del comando `EVENTS` . Risulta utile per visualizzare le informazioni su vari eventi.

4.10.2.1 Contesto - AV

ANTI-STEALTH

Attiva Anti-Stealth.

SINTASSI:

```
[get] | restore antistealth
```

```
set antistealth disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

CLEANLEVEL

Livello di pulitura.

SINTASSI:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non pulire

`normal` - Pulitura standard

`strict` - Massima pulitura

ESCLUSIONI

Esclusioni.

SINTASSI:

```
[get] | clear exclusions
```

```
add | remove exclusions <exclusion>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`exclusion` - File/cartella/maschera esclusi

EXTENSIONS

Estensioni controllate/escluse.

SINTASSI:

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`extension` - Estensione

`all` - Tutti i file

`extless` - File senza estensione

AUTOPROTEZIONE

Autoprotezione.

SINTASSI:

```
[get] | restore selfdefense
```

```
set selfdefense disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

STATUS

Stato della protezione antivirus.

SINTASSI:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAZIONI:

`get` - Mostra lo stato della protezione antivirus

`set` - Disattiva/attiva la protezione antivirus

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la protezione antivirus

`enabled` - Attiva la protezione antivirus

4.10.2.2 Contesto - AV DOCUMENT

CLEANLEVEL

Livello di pulitura.

SINTASSI:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non pulire

`normal` - Pulitura standard

`strict` - Massima pulitura

EXTENSIONS

Estensioni controllate/escluse.

SINTASSI:

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`extension` - Estensione

`all` - Tutti i file

`extless` - File senza estensione

INTEGRATION

Integra protezione documenti nel sistema.

SINTASSI:

```
[get] | restore integration
```

`set integration disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

STATUS

Stato di protezione corrente del documento.

SINTASSI:

`[get] | restore status`

`set status disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.3 Contesto - AV DOCUMENT LIMITS ARCHIVE

LEVEL

Livello di ricerca negli archivi.

SINTASSI:

`[get] | restore level`

`set level <number>`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Livello da 1 a 20 oppure 0 per le impostazioni predefinite

SIZE

Dimensione massima file in archivio (kB).

SINTASSI:

`[get] | restore size`

`set size <number>`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB (1 - 3145728) oppure 0 per le impostazioni predefinite

4.10.2.4 Contesto - AV DOCUMENT LIMITS OBJECTS

SIZE

Dimensione massima dell'archivio (kB)

SINTASSI:

```
[get] | restore size
```

```
set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB (1 - 3145728) oppure 0 per le impostazioni predefinite

TIMEOUT

Tempo massimo del controllo per gli archivi (sec.)

SINTASSI:

```
[get] | restore timeout
```

```
set timeout <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Tempo in secondi (1 - 3600) oppure 0 per le impostazioni predefinite

4.10.2.5 Contesto - AV DOCUMENT OBJECTS

ARCHIVE

Controlla archivi.

SINTASSI:

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

BOOT

Controlla settori di avvio.

SINTASSI:

```
[get] | restore boot

set boot disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EMAIL

Controlla file e-mail.

SINTASSI:

```
[get] | restore email

set email disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

FILE

Controlla file.

SINTASSI:

```
[get] | restore file

set file disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

MEMORY

Controlla memoria.

SINTASSI:

```
[get] | restore memory

set memory disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RUNTIME

Controlla eseguibili compressi.

SINTASSI:

```
[get] | restore runtime

set runtime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SFX

Controlla archivi autoestraenti.

SINTASSI:

```
[get] | restore sfx

set sfx disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.6 Contesto - AV DOCUMENT OPTIONS

ADVHEURISTICS

Utilizza euristica avanzata.

SINTASSI:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

ADWARE

Rilevamento di adware/spyware/riskware.

SINTASSI:

```
[get] | restore adware
set adware disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HEURISTICS

Utilizza euristica.

SINTASSI:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SIGNATURES

Utilizza firme.

SINTASSI:

```
[get] | restore signatures
```

```
set signatures disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNSAFE

Rilevamento delle applicazioni potenzialmente pericolose.

SINTASSI:

```
[get] | restore unsafe
```

```
set unsafe disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNWANTED

Rilevamento delle applicazioni potenzialmente indesiderate.

SINTASSI:

```
[get] | restore unwanted
```

```
set unwanted disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.7 Contesto - AV DOCUMENT OTHER

LOGALL

Registra tutti gli oggetti.

SINTASSI:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPTIMIZE

Ottimizzazione Smart.

SINTASSI:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.8 Contesto - AV EMAIL

AZIONE

Azione per messaggi infetti.

SINTASSI:

```
[get] | restore action
```

```
set action none | delete | movedeleted | moveto
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Nessuna azione

`delete` - Elimina il messaggio

`movedeleted` - Sposta nella cartella eliminati

`moveto` - Sposta nella cartella

CLIENTS

Client di posta.

SINTASSI:

```
[get] clients

add | remove clients <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`path` - Percorso delle applicazioni

NOTA: solo con il filtraggio per applicazione è necessario specificare le applicazioni che verranno utilizzate come client di posta. Se un'applicazione non viene contrassegnata come client di posta, l'e-mail potrebbe non essere controllata.

QUARANTINE

Cartella messaggi infetti.

SINTASSI:

```
[get] | restore quarantine

set quarantine <string>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome cartella

STATUS

Stato della protezione client di posta.

SINTASSI:

```
[get] | restore status

set status disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.9 Contesto - AV EMAIL GENERAL

CLEANLEVEL

Livello di pulitura.

SINTASSI:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non pulire

`normal` - Pulitura standard

`strict` - Massima pulitura

EXTENSIONS

Estensioni controllate/escluse.

SINTASSI:

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`extension` - Estensione

`all` - Tutti i file

`extless` - File senza estensione

4.10.2.10 Contesto - AV EMAIL GENERAL LIMITS ARCHIVE

LEVEL

Livello di ricerca negli archivi.

SINTASSI:

```
[get] | restore level
```

```
set level <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Livello da 1 a 20 oppure 0 per le impostazioni predefinite

SIZE

Dimensione massima file in archivio (kB).

SINTASSI:

```
[get] | restore size
```

```
set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

4.10.2.11 Contesto - AV EMAIL GENERAL LIMITS OBJECTS

SIZE

Dimensione massima dell'archivio (kB).

SINTASSI:

```
[get] | restore size
```

```
set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

TIMEOUT

Tempo massimo del controllo per gli archivi (sec.).

SINTASSI:

```
[get] | restore timeout
```

```
set timeout <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Tempo in secondi oppure 0 per le impostazioni predefinite

4.10.2.12 Contesto - AV EMAIL GENERAL OBJECTS

ARCHIVE

Controlla archivi.

SINTASSI:

```
[get] | restore archive
set archive disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

BOOT

Controlla settori di avvio.

SINTASSI:

```
[get] | restore boot
set boot disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EMAIL

Controlla file e-mail.

SINTASSI:

```
[get] | restore email
set email disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

FILE

Controlla file.

SINTASSI:

```
[get] | restore file

set file disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

MEMORY

Controlla memoria.

SINTASSI:

```
[get] | restore memory

set memory disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RUNTIME

Controlla eseguibili compressi.

SINTASSI:

```
[get] | restore runtime

set runtime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SFX

Controlla archivi autoestraenti.

SINTASSI:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.13 Contesto - AV EMAIL GENERAL OPTIONS

ADVHEURISTICS

Utilizza euristica avanzata.

SINTASSI:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

ADWARE

Rilevamento di adware/spyware/riskware.

SINTASSI:

```
[get] | restore adware
set adware disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HEURISTICS

Utilizza euristica.

SINTASSI:

```
[get] | restore heuristics
```

`set heuristics disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SIGNATURES

Utilizza firme.

SINTASSI:

`[get] | restore signatures`

`set signatures disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNSAFE

Rilevamento delle applicazioni potenzialmente pericolose.

SINTASSI:

`[get] | restore unsafe`

`set unsafe disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNWANTED

Rilevamento delle applicazioni potenzialmente indesiderate.

SINTASSI:

`[get] | restore unwanted`

`set unwanted disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.14 Contesto - AV EMAIL GENERAL OTHER

LOGALL

Registra tutti gli oggetti.

SINTASSI:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPTIMIZE

Ottimizzazione Smart.

SINTASSI:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.15 Contesto - AV EMAIL MESSAGE CONVERT PLAIN

Converti testo e-mail in testo semplice.

SINTASSI:

```
[get] | restore plain

set plain disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.16 Contesto - AV EMAIL MODIFY TEMPLATE

Template aggiunto all'oggetto dei messaggi infetti.

SINTASSI:

```
[get] | restore template

set template [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Testo

4.10.2.17 Contesto - AV EMAIL MODIFY RECEIVED BODY

Aggiungi notifiche alle e-mail ricevute e lette.

SINTASSI:

```
[get] | restore body

set body never | infected | all
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`never` - Non aggiungere

`infected` - Solo ai messaggi infetti

`all` - A tutti i messaggi

SUBJECT

Aggiungi nota all'oggetto di e-mail infette ricevute e inviate.

SINTASSI:

```
[get] | restore subject

set subject disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.18 Contesto - AV EMAIL MODIFY SENT BODY

Aggiungi notifiche alle e-mail ricevute e lette.

SINTASSI:

```
[get] | restore body

set body never | infected | all
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`never` - Non aggiungere

`infected` - Solo ai messaggi infetti

`all` - A tutti i messaggi

SUBJECT

Aggiungi nota all'oggetto di e-mail infette ricevute e inviate.

SINTASSI:

```
[get] | restore subject

set subject disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.19 Contesto - AV EMAIL OEXPRESS/WINMAIL

INTEGRATION

Integra con Outlook Express e Windows Mail.

SINTASSI:

```
[get] | restore integration
set integration disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.20 Contesto - AV EMAIL OUTLOOK

FORCEADDIN

Utilizzare COM Add-in nelle versioni precedenti di Microsoft Outlook.

SINTASSI:

```
[get] | restore forceaddin
set forceaddin 2010newer | 2007newer | allversions
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`2010newer` - Microsoft Outlook 2010 e versioni successive

`2007newer` - Microsoft Outlook 2007 e versioni successive

`allversions` - Tutte le versioni Microsoft Outlook

INTEGRATION

Integra con Microsoft Outlook.

SINTASSI:

```
[get] | restore integration
set integration disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SYNCFIX

Attiva la risoluzione dei conflitti di sincronizzazione in Microsoft Outlook.

SINTASSI:

```
[get] | restore syncfix
```

```
set syncfix <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

`0` - Disattivata, `3` - Completamente attivata, altri valori possibili.

4.10.2.21 Contesto - AV EMAIL OUTLOOK RESCAN

ONCHANGE

Disattiva il controllo alla modifica del contenuto della posta in arrivo.

SINTASSI:

```
[get] | restore onchange
```

```
set onchange disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.22 Contesto - AV EMAIL PROTOCOL POP3

COMPATIBILITY

Configurazione della compatibilità.

SINTASSI:

```
[get] | restore compatibility
```

```
set compatibility compatible | both | effective
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`compatible` - Livello di compatibilità massima

`both` - Livello di compatibilità media

`effective` - Efficienza massima

NOTA: Non tutti i client di posta potrebbero funzionare correttamente insieme al filtraggio POP3 nella modalità standard. Le seguenti impostazioni consentono di regolare il livello di compatibilità per risolvere possibili conflitti. L'aumento del livello di compatibilità potrebbe tuttavia causare una riduzione dell'efficacia del monitoraggio Internet o instabilità per poterne sfruttare tutte le funzionalità.

PORTS

Porte utilizzate da POP3.

SINTASSI:

```
[get] | restore ports

set ports [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Numeri porte separati da una virgola

USE

Controlla POP3.

SINTASSI:

```
[get] | restore use

set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.23 Contesto - AV EMAIL PROTOCOL POP3S

COMPATIBILITY

Configurazione della compatibilità.

SINTASSI:

```
[get] | restore compatibility

set compatibility compatible | both | effective
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`compatible` - Livello di compatibilità massima

`both` - Livello di compatibilità media

`effective` - Efficienza massima

NOTA: Non tutti i client di posta potrebbero funzionare correttamente insieme al filtraggio POP3S nella modalità standard. Le seguenti impostazioni consentono di regolare il livello di compatibilità per risolvere possibili conflitti. L'aumento del livello di compatibilità potrebbe tuttavia causare una riduzione dell'efficacia del monitoraggio Internet o instabilità per poterne sfruttare tutte le funzionalità.

MODE

Modalità di filtraggio POP3S.

SINTASSI:

```
[get] | restore mode

set mode none | ports | clients
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non effettuare il controllo protocollo POP3S

`ports` - Effettua controllo protocollo POP3S per le porte selezionate

`clients` - Effettua controllo protocollo POP3S per applicazioni contrassegnate come client di posta che utilizzano le porte selezionate

PORTS

Porte utilizzate da POP3S.

SINTASSI:

```
[get] | restore ports

set ports [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Numeri porte separati da una virgola

4.10.2.24 Contesto - AV EMAIL RESCAN

ONUPDATE

Ripeti controllo dopo l'aggiornamento.

SINTASSI:

```
[get] | restore onupdate
```

```
set onupdate disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.25 Contesto - AV EMAIL SCAN

OTHERMODULES

Accetta i risultati del controllo da altri moduli.

SINTASSI:

```
[get] | restore othermodules
```

```
set othermodules disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

PLAIN

Controlla corpo e-mail testo semplice.

SINTASSI:

```
[get] | restore plain
```

```
set plain disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

READ

Controlla messaggi letti.

SINTASSI:

```
[get] | restore read

set read disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RECEIVED

Controlla messaggi ricevuti.

SINTASSI:

```
[get] | restore received

set received disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RTF

Controlla corpo e-mail RTF.

SINTASSI:

```
[get] | restore rtf

set rtf disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SENT

Controlla messaggi inviati.

SINTASSI:

```
[get] | restore sent

set sent disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.26 Contesto - AV EMAIL THUNDERBIRD INTEGRATION

Integra con Mozilla Thunderbird.

SINTASSI:

```
[get] | restore integration

set integration disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.27 Contesto - AV EMAIL WINLIVE INTEGRATION

Integra con Windows Live Mail.

SINTASSI:

```
[get] | restore integration

set integration disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.28 Contesto - AV LIMITS ARCHIVE

LEVEL

Livello di ricerca negli archivi.

SINTASSI:

```
[get] | restore level

set level <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Livello da 1 a 20 oppure 0 per le impostazioni predefinite

SIZE

Dimensione massima file in archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

4.10.2.29 Contesto - AV LIMITS OBJECTS

SIZE

Dimensione massima dell'archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

TIMEOUT

Tempo massimo del controllo per gli archivi (sec.).

SINTASSI:

```
[get] | restore timeout
```

```
set timeout <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Tempo in secondi oppure 0 per le impostazioni predefinite

4.10.2.30 Contesto - AV NETFILTER

AUTOSTART

Esegui automaticamente il filtraggio del contenuto dei protocolli di applicazioni HTTP e POP3.

SINTASSI:

```
[get] | restore autostart
```

```
set autostart disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EXCLUDED

Applicazioni escluse dal filtraggio protocolli.

SINTASSI:

```
[get] excluded
```

```
add | remove excluded <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`path` - Percorso delle applicazioni

MODE

Reindirizza traffico per il filtraggio.

SINTASSI:

```
[get] | restore mode
```

```
set mode ports | application | both
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`ports` - Porte HTTP e POP3

`application` - Applicazioni contrassegnate come browser Web o client di posta

`both` - Porte e applicazioni contrassegnate come browser Web o client di posta

STATUS

Attiva filtraggio dei contenuti dei protocolli di applicazioni HTTP e POP3.

SINTASSI:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.31 Contesto - AV NETFILTER PROTOCOL SSL

BLOCKSSL2

Blocca comunicazioni crittografate che utilizzano il protocollo obsoleto SSL v2.

SINTASSI:

```
[get] | restore blockssl2
```

```
set blockssl2 disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EXCEPTIONS

Applica le eccezioni create in base ai certificati.

SINTASSI:

```
[get] | restore exceptions
```

```
set exceptions disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

MODE

Modalità filtraggio SSL.

SINTASSI:

```
[get] | restore mode
```

```
set mode allways | ask | none
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`allways` - Effettua sempre il controllo SSL

`ask` - Chiedi conferma per siti non visitati (è possibile configurare esclusioni)

`none` - Non effettuare il controllo del protocollo SSL

4.10.2.32 Contesto - AV NETFILTER PROTOCOL SSL CERTIFICATE

ADDTOBROWSERS

Aggiungi il certificato radice ai browser conosciuti.

SINTASSI:

```
[get] | restore addtobrowsers
```

```
set addtobrowsers disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

NOTA: Per controllare correttamente il traffico codificato con SSL, il certificato radice per ESET, spol. s r.o usato per firmare i certificati, sarà aggiunto all'Archivio Autorità di certificazione radice attendibili (TRCA).

EXCLUDED

Elenco di certificati esclusi dal filtraggio dei contenuti.

SINTASSI:

```
[get] excluded
```

```
 remove excluded <name>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`remove` - Rimuove voce

ARGOMENTI:

`name` - Nome del certificato

NOTTRUSTED

Non attendibile se il certificato è danneggiato o non valido.

SINTASSI:

```
[get] | restore nottrusted
```

```
set nottrusted ask | block
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`ask` - Chiedi conferma della validità dei certificati

`block` - Blocca comunicazioni che utilizzano il certificato

TRUSTED

Elenco certificati attendibili.

SINTASSI:

```
[get] trusted
```

```
remove trusted <name>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`remove` - Rimuove voce

ARGOMENTI:

`name` - Nome del certificato

UNKNOWNROOT

Radice sconosciuta - Se il certificato non può essere verificato utilizzando il TRCA.

SINTASSI:

```
[get] | restore unknownroot
```

```
set unknownroot ask | block
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`ask` - Chiedi conferma della validità dei certificati

`block` - Blocca comunicazioni che utilizzano il certificato

4.10.2.33 Contesto - AV OBJECTS

ARCHIVE

Controlla archivi.

SINTASSI:

```
[get] | restore archive

set archive disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

BOOT

Controlla settori di avvio.

SINTASSI:

```
[get] | restore boot

set boot disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EMAIL

Controlla file e-mail.

SINTASSI:

```
[get] | restore email

set email disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

MEMORY

Controlla memoria.

SINTASSI:

```
[get] | restore memory

set memory disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RUNTIME

Controlla eseguibili compressi.

SINTASSI:

```
[get] | restore runtime

set runtime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SFX

Controlla archivi autoestraenti.

SINTASSI:

```
[get] | restore sfx

set sfx disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.34 Contesto - AV OPTIONS

ADVHEURISTICS

Utilizza euristica avanzata.

SINTASSI:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HEURISTICS

Utilizza euristica.

SINTASSI:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNSAFE

Rilevamento delle applicazioni potenzialmente pericolose.

SINTASSI:

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNWANTED

Rilevamento delle applicazioni potenzialmente indesiderate.

SINTASSI:

```
[get] | restore unwanted

set unwanted disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.35 Contesto - AV OTHER

LOGALL

Registra tutti gli oggetti.

SINTASSI:

```
[get] | restore logall

set logall disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPTIMIZE

Ottimizzazione Smart.

SINTASSI:

```
[get] | restore optimize

set optimize disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.36 Contesto - AV REALTIME

AUTOSTART

Avvia automaticamente la protezione in tempo reale.

SINTASSI:

```
[get] | restore autostart
set autostart disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

CLEANLEVEL

Livello di pulitura

SINTASSI:

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non pulire

`normal` - Pulitura standard

`strict` - Massima pulitura

EXTENSIONS

Estensioni controllate/escluse.

SINTASSI:

```
[get] | restore extensions
add | remove extensions <extension> | /all | /extless
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`extension` - Estensione

`all` - Tutti i file

`extless` - File senza estensione

STATUS

Stato protezione computer in tempo reale.

SINTASSI:

```
[get] | restore status

set status disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.37 Contesto - AV REALTIME DISK

FLOPPY

Controlla supporti rimovibili.

SINTASSI:

```
[get] | restore floppy

set floppy disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

LOCAL

Controlla unità locali.

SINTASSI:

```
[get] | restore local

set local disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

NETWORK

Controlla unità di rete.

SINTASSI:

```
[get] | restore network
```

```
set network disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.38 Contesto - AV REALTIME EVENT

CREATE

Controlla file alla creazione.

SINTASSI:

```
[get] | restore create
```

```
set create disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EXECUTE

Controlla file all'esecuzione.

SINTASSI:

```
[get] | restore execute
```

```
set execute disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

FLOPPYACCESS

Esegui controllo all'accesso ai dischetti.

SINTASSI:

```
[get] | restore floppyaccess
```

```
set floppyaccess disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPEN

Controlla file all'apertura.

SINTASSI:

```
[get] | restore open
```

```
set open disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SHUTDOWN

Esegui controllo all'arresto del computer.

SINTASSI:

```
[get] | restore shutdown
```

```
set shutdown disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.39 Contesto - AV REALTIME EXECUTABLE

ADVHEURISTICS

Attiva euristica avanzata all'esecuzione dei file.

SINTASSI:

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.40 Contesto - AV REALTIME EXECUTABLE FROMREMOVABLE

ADVHEURISTICS

Attiva euristica avanzata all'esecuzione dei file dai supporti rimovibili.

SINTASSI:

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EXCLUSION

Esclusioni unità USB.

SINTASSI:

```
[get] | restore exclusion
```

```
select exclusion none | <drive> | all
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`select` - Seleziona voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Deseleziona tutte le unità

`drive` - Lettera di un'unità da selezionare/deselezionare

`all` - Seleziona tutte le unità

NOTA: usare questa opzione per consentire le eccezioni dal controllo tramite l'euristica avanzata all'esecuzione dei file. Le configurazioni dell'euristica avanzata per le unità del disco rigido saranno applicate ai dispositivi selezionati.

4.10.2.41 Contesto - AV REALTIME LIMITS ARCHIVE

LEVEL

Livello di ricerca negli archivi.

SINTASSI:

```
[get] | restore level

set level <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Livello da 1 a 20 oppure 0 per le impostazioni predefinite

SIZE

Dimensione massima file in archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

4.10.2.42 Contesto - AV REALTIME LIMITS OBJECTS

SIZE

Dimensione massima dell'archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

TIMEOUT

Tempo massimo del controllo per gli archivi (sec.).

SINTASSI:

```
[get] | restore timeout

set timeout <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Tempo in secondi oppure 0 per le impostazioni predefinite

4.10.2.43 Contesto - AV REALTIME OBJECTS

ARCHIVE

Controlla archivi.

SINTASSI:

```
[get] | restore archive

set archive disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

BOOT

Controlla settori di avvio.

SINTASSI:

```
[get] | restore boot

set boot disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EMAIL

Controlla file e-mail.

SINTASSI:

```
[get] | restore email
```

```
set email disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

MEMORY

Controlla memoria.

SINTASSI:

```
[get] | restore memory
```

```
set memory disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RUNTIME

Controlla eseguibili compressi.

SINTASSI:

```
[get] | restore runtime
```

```
set runtime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SFX

Controlla archivi autoestraenti.

SINTASSI:

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.44 Contesto - AV REALTIME ONWRITE

ADVHEURISTICS

Attiva euristica avanzata per file nuovi e modificati.

SINTASSI:

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RUNTIME

Controlla archivi di esecuzione nuovi e modificati.

SINTASSI:

```
[get] | restore runtime
```

```
set runtime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SFX

Controlla archivi autoestraenti nuovi e modificati.

SINTASSI:

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.45 Contesto - AV REALTIME ONWRITE ARCHIVE

LEVEL

Livello di ricerca approfondita negli archivi.

SINTASSI:

```
[get] | restore level
```

```
set level <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Livello (0 - 20)

SIZE

Dimensione massima di un file in archivio controllato (kB).

SINTASSI:

```
[get] | restore size
```

```
set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione (kB)

4.10.2.46 Contesto - AV REALTIME OPTIONS

ADVHEURISTICS

Utilizza euristica avanzata.

SINTASSI:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HEURISTICS

Utilizza euristica.

SINTASSI:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNSAFE

Rilevamento delle applicazioni potenzialmente pericolose.

SINTASSI:

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNWANTED

Rilevamento delle applicazioni potenzialmente indesiderate.

SINTASSI:

```
[get] | restore unwanted

set unwanted disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.47 Contesto - AV REALTIME OTHER

LOGALL

Registra tutti gli oggetti.

SINTASSI:

```
[get] | restore logall

set logall disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPTIMIZE

Ottimizzazione Smart.

SINTASSI:

```
[get] | restore optimize

set optimize disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.48 Contesto - AV REALTIME REMOVABLE

BLOCK

Blocca supporti rimovibili.

SINTASSI:

```
[get] | restore block
```

```
set block disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EXCLUSION

Supporti rimovibili consentiti.

SINTASSI:

```
[get] | restore exclusion
```

```
select exclusion none | <drive> | all
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`select` - Seleziona voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Deseleziona tutte le unità

`drive` - Lettera di un'unità da selezionare/deselezionare

`all` - Seleziona tutte le unità

NOTA: usare questa opzione per attivare l'accesso ai supporti rimovibili (CD, dischetti, unità USB). Quando si seleziona un supporto, si rimuovono le restrizioni di accesso quando si tenta di accedere a tale supporto specifico.

4.10.2.49 Contesto - AV WEB

BROWSERS

Browser Web.

SINTASSI:

```
[get] browsers
```

```
add | remove browsers <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`path` - Percorso delle applicazioni

NOTA: per aumentare la protezione, si consiglia di contrassegnare le applicazioni utilizzate come browser Internet selezionando la casella appropriata. Se un'applicazione non viene contrassegnata come browser Web, è possibile che i dati trasferiti tramite tale applicazione non vengano controllati.

CLEANLEVEL

Livello di pulitura.

SINTASSI:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non pulire

`normal` - Pulitura standard

`strict` - Massima pulitura

EXTENSIONS

Estensioni controllate/escluse.

SINTASSI:

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`extension` - Estensione

`all` - Tutti i file

`extless` - File senza estensione

STATUS

Protezione accesso Web.

SINTASSI:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.50 Contesto - AV WEB ADDRESSMGMT

ADDRESS

Gestione indirizzi nell'elenco selezionato.

SINTASSI:

```
[get] | clear address
add | remove address <address>
import | export address <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`import` - Importa da file

`export` - Esporta in un file

`clear` - Rimuove tutti gli elementi/file

ARGOMENTI:

`address` - Indirizzo

`path` - Percorso file

LIST

Gestione elenchi indirizzi.

SINTASSI:

```
[get] | restore list
set list <listname> disabled | enabled
select | remove list <listname>
add list allowed <listname> | blocked <listname> | excluded <listname>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`select` - Seleziona per la modifica

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`listname` - Nome elenco

`disabled` - Non usare elenco

`enabled` - Utilizza elenco

`allowed` - Elenco di indirizzi consentiti

`blocked` - Elenco di indirizzi bloccati

`excluded` - Elenco indirizzi esclusi dal filtro

NOTA: per modificare l'elenco selezionato (contrassegnato con - x) utilizzare il comando `av web addressmgmt address` .

NOTIFY

Notifica all'applicazione di indirizzi nell'elenco.

SINTASSI:

```
[get] | restore notify
```

```
set notify disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

WHITELISTED

Consenti accesso solo a indirizzi HTTP nell'elenco di indirizzi consentiti.

SINTASSI:

```
[get] | restore whitelisted
```

```
set whitelisted disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.51 Contesto - AV WEB LIMITS ARCHIVE

LEVEL

Livello di ricerca negli archivi.

SINTASSI:

```
[get] | restore level
```

```
set level <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Livello da 1 a 20 oppure 0 per le impostazioni predefinite

SIZE

Dimensione massima file in archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

4.10.2.52 Contesto - AV WEB LIMITS OBJECTS

SIZE

Dimensione massima dell'archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

TIMEOUT

Tempo massimo del controllo per gli archivi (sec.).

SINTASSI:

```
[get] | restore timeout

set timeout <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Tempo in secondi oppure 0 per le impostazioni predefinite

4.10.2.53 Contesto - AV WEB OBJECTS

ARCHIVE

Controlla archivi.

SINTASSI:

```
[get] | restore archive

set archive disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

BOOT

Controlla settori di avvio.

SINTASSI:

```
[get] | restore boot

set boot disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EMAIL

Controlla file e-mail.

SINTASSI:

```
[get] | restore email

set email disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

FILE

Controlla file.

SINTASSI:

```
[get] | restore file

set file disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

MEMORY

Controlla memoria.

SINTASSI:

```
[get] | restore memory

set memory disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RUNTIME

Controlla eseguibili compressi.

SINTASSI:

```
[get] | restore runtime

set runtime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SFX

Controlla archivi autoestraenti.

SINTASSI:

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.54 Contesto - AV WEB OPTIONS

ADVHEURISTICS

Utilizza euristica avanzata.

SINTASSI:

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

ADWARE

Rilevamento di adware/spyware/riskware.

SINTASSI:

```
[get] | restore adware
```

```
set adware disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HEURISTICS

Utilizza euristica.

SINTASSI:

```
[get] | restore heuristics
```

`set heuristics disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SIGNATURES

Utilizza firme.

SINTASSI:

`[get] | restore signatures`

`set signatures disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNSAFE

Rilevamento delle applicazioni potenzialmente pericolose.

SINTASSI:

`[get] | restore unsafe`

`set unsafe disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNWANTED

Rilevamento delle applicazioni potenzialmente indesiderate.

SINTASSI:

`[get] | restore unwanted`

`set unwanted disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.55 Contesto - AV WEB OPTIONS BROWSERS

ACTIVEMODE

Modalità attiva per i browser Web.

SINTASSI:

```
[get] activemode
```

```
add | remove activemode <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`path` - Percorso delle applicazioni

NOTA: i programmi aggiunti all'elenco vengono aggiunti automaticamente all'elenco dei browser Web.

4.10.2.56 Contesto - AV WEB OTHER

LOGALL

Registra tutti gli oggetti.

SINTASSI:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPTIMIZE

Ottimizzazione Smart.

SINTASSI:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.57 Contesto - AV WEB PROTOCOL HTTP

PORTS

Porte utilizzate dal protocollo HTTP.

SINTASSI:

```
[get] | restore ports
```

```
set ports [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Numeri di porta separati mediante virgola

USE

Controllo HTTP.

SINTASSI:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.58 Contesto - AV WEB PROTOCOL HTTPS

MODE

Modalità di filtraggio HTTPS.

SINTASSI:

```
[get] | restore mode
```

```
set mode none | ports | browsers
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non effettuare il controllo protocollo

`ports` - Effettua controllo protocollo HTTPS per le porte selezionate

`browsers` - Effettua controllo protocollo HTTPS per applicazioni contrassegnate come browser Web che utilizzano le porte selezionate

PORTS

Porte utilizzate dal protocollo HTTPS.

SINTASSI:

```
[get] | restore ports
```

```
set ports [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Numeri porte separati da una virgola

4.10.2.59 Contesto - GENERAL

CONFIG

Importa/esporta impostazioni.

SINTASSI:

```
import | export config <path>
```

OPERAZIONI:

`import` - Importa da file

`export` - Esporta in un file

ARGOMENTI:

`path` - Percorso file

LICENSE

Gestione delle licenze.

SINTASSI:

```
[get] license

import license <path>

export license <ID> <path>

remove license <ID>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`remove` - Rimuove voce

`import` - Importa da file

`export` - Esporta in un file

ARGOMENTI:

`path` - Percorso dei file di licenza

`ID` - ID licenza

4.10.2.60 Contesto - GENERAL ACCESS

ADMIN

Protezione impostazioni diritti amministratore.

SINTASSI:

```
[get] | restore admin

set admin disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

BATCH

Esegui comandi immessi come argomenti quando eShell è in esecuzione.

SINTASSI:

```
[get] | restore batch

set batch disabled | <time> | allways
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattivato

`time` - Intervallo di tempo in minuti (1 - 1440 minuti)

`always` - Sempre

PASSWORD

Questa password viene utilizzata per i comandi protetti con password. In genere, per eseguire comandi protetti con password, all'utente viene chiesto di immettere una password. Tale richiesta assicura la protezione. Ciò è applicabile a comandi che disattivano la protezione antivirus o che potrebbero influenzare la funzionalità di ESET File Security. A ogni esecuzione di tale comando, all'utente verrà chiesto di inserire la password. In alternativa, è possibile definire tale password per la sessione eShell corrente e non verrà chiesto di inserirla nuovamente. Per ulteriori informazioni, fare clic qui.

Per l'immissione interattiva della password (consigliata), lasciare vuoti i parametri. Per reimpostare la password, immettere una password vuota.

PERCORSO CONTESTUALE:

```
accesso generale
```

SINTASSI:

```
[get] | restore | set password
```

OPERAZIONI:

`get` - Mostra password

`set` - Imposta password

`restore` - Ripristina password

ESEMPI:

`get password` - Utilizzare questo comando per visualizzare se la password è configurata o meno (verranno visualizzati solo asterischi "*" e non la password stessa). Se non sono visibili asterischi, significa che la password non è impostata

`set password` - Utilizzare questo comando per impostare la password: è sufficiente immetterla (se non si immette la password, la protezione delle impostazioni non viene utilizzata)

`restore password` - Questo comando consente di cancellare la password esistente (la protezione delle impostazioni non verrà utilizzata)

EQUIVALENTE GUI:

per visualizzare come viene configurato questo comando tramite l'interfaccia utente, fare clic qui.

4.10.2.61 Contesto - GENERAL ESHELL

ALIAS

Gestione alias.

SINTASSI:

```
[get] | clear | restore alias
```

```
add alias [.] <alias>=<command>
```

```
remove alias <alias>
```

```
import | export alias <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`import` - Importa da file

`export` - Esporta in un file

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`.` - Crea alias globali

`alias` - Nuovo alias

`command` - Comando associato (validità del comando non controllata)

`alias` - Alias da eliminare

`path` - Percorso file

LISTER

Utilizza creatore elenco.

SINTASSI:

```
[get] | restore lister
```

```
set lister disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.62 Contesto - GENERAL ESHELL COLOR

ALIAS

Colore alias.

SINTASSI:

```
[get] | restore alias
```

```
set alias [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

COMMAND

Colore comando.

SINTASSI:

```
[get] | restore command
```

```
set command [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

CONTEXT

Colore contesto.

SINTASSI:

```
[get] | restore context

set context [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

DEFAULT

Colore base.

SINTASSI:

```
[get] | restore default

set default [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

DISABLED

Colore N/D.

SINTASSI:

```
[get] | restore disabled
```

```
set disabled [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

ERROR

Colore dei messaggi di errore.

SINTASSI:

```
[get] | restore error
```

```
set error [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

INTERACTIVE

Colore delle operazioni interattive.

SINTASSI:

```
[get] | restore interactive
```

```
set interactive [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

LIST1

Colore elenco 1.

SINTASSI:

```
[get] | restore list1
```

```
set list1 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red |
magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

LIST2

Colore elenco 2.

SINTASSI:

```
[get] | restore list2
```

```
set list2 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

SUCCESS

Colore OK stato.

SINTASSI:

```
[get] | restore success
```

```
set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

WARNING

Colore dei messaggi di avviso.

SINTASSI:

```
[get] | restore warning

set warning [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`black` - Nero

`navy` - Blu navy

`grass` - Verde prato

`ltblue` - Celeste

`brown` - Marrone

`purple` - Viola

`olive` - Verde oliva

`ltgray` - Grigio chiaro

`gray` - Grigio

`blue` - Blu

`green` - Verde

`cyan` - Ciano

`red` - Rosso

`magenta` - Magenta

`yellow` - Giallo

`white` - Bianco

4.10.2.63 Contesto - GENERAL ESHELL OUTPUT

UTF8

Output codificato UTF8.

SINTASSI:

```
[get] | restore utf8
```

```
set utf8 disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

NOTA: per una visualizzazione corretta, la riga di comando dovrebbe utilizzare un carattere TrueType quale ad esempio 'Lucida Console'.

4.10.2.64 Contesto - GENERAL ESHELL STARTUP

LOADCOMMANDS

Carica tutti i comandi all'avvio.

SINTASSI:

```
[get] | restore loadcommands
```

```
set loadcommands disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

STATUS

Mostra lo stato di protezione all'avvio.

SINTASSI:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.65 Contesto - GENERAL ESHELL VIEW

CMDHELP

Mostra la Guida in caso di errore del comando.

SINTASSI:

```
[get] | restore cmdhelp
```

```
set cmdhelp disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

COLORS

Utilizza colori.

SINTASSI:

```
[get] | restore colors
```

```
set colors disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

FITWIDTH

Taglia testo per adattarlo alla larghezza.

SINTASSI:

```
[get] | restore fitwidth
```

```
set fitwidth disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

GLOBAL

Mostra i comandi globali.

SINTASSI:

```
[get] | restore global
```

```
set global disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HIDDEN

Visualizza i comandi nascosti.

SINTASSI:

```
[get] | restore hidden
```

```
set hidden disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPERATIONS

Mostra le operazioni nell'elenco dei comandi.

SINTASSI:

```
[get] | restore operations
```

```
set operations disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SHORTLIST

Mostra l'elenco dei comandi brevi alla modifica del contesto.

SINTASSI:

```
[get] | restore shortlist
```

```
set shortlist disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SYNTAXHINT

Mostra suggerimenti sulla sintassi dei comandi.

SINTASSI:

```
[get] | restore syntaxhint
```

```
set syntaxhint disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

VALUESONLY

Visualizza valori senza descrizione.

SINTASSI:

```
[get] | restore valuesonly
```

```
set valuesonly disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.66 Contesto - GENERAL PERFORMANCE

SCANNERS

Numero di controlli in esecuzione.

SINTASSI:

```
[get] | restore scanners
```

```
set scanners <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Conteggio (1 - 20)

4.10.2.67 Contesto - GENERAL PROXY

ADDRESS

Indirizzo server proxy.

SINTASSI:

```
[get] | restore address
```

```
set address [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo

DETECT

Rileva configurazione del server proxy.

SINTASSI:

```
detect
```

LOGIN

Nome accesso.

SINTASSI:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome

PASSWORD

Password del server proxy.

SINTASSI:

```
[get] | restore password

set password [plain <password>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

PORT

Porta

SINTASSI:

```
[get] | restore port

set port <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Numero di porta.

USE

Utilizza server proxy.

SINTASSI:

```
[get] | restore use

set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.68 Contesto - GENERAL QUARANTINE RESCAN UPDATE

Ripeti controllo dei file in quarantena dopo ogni aggiornamento.

SINTASSI:

```
[get] | restore update
```

```
set update disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

restore - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.69 Contesto - GENERAL REMOTE INTERVAL

Intervallo di connessione (minuti).

SINTASSI:

```
[get] | restore interval
```

```
set interval <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Tempo in minuti (1 - 1440)

USE

Connessione server ERA.

SINTASSI:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.70 Contesto - GENERAL REMOTE SERVER PRIMARY

ADDRESS

Indirizzo server ERA.

SINTASSI:

```
[get] | restore address
```

```
set address [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo

ENCRYPT

Blocca connessione non crittografata.

SINTASSI:

```
[get] | restore encrypt
```

```
set encrypt disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

PASSWORD

Password server ERA.

SINTASSI:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

PORT

Porta server ERA.

SINTASSI:

```
[get] | restore port

set port <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Numero di porta.

4.10.2.71 Contesto - GENERAL REMOTE SERVER SECONDARY

ADDRESS

Indirizzo server ERA.

SINTASSI:

```
[get] | restore address

set address [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo

ENCRYPT

Blocca connessione non crittografata.

SINTASSI:

```
[get] | restore encrypt

set encrypt disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

PASSWORD

Password server ERA.

SINTASSI:

```
[get] | restore password
set password [plain <password>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

PORT

Porta server ERA.

SINTASSI:

```
[get] | restore port
set port <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Numero di porta.

4.10.2.72 Contesto - GENERAL TS.NET

EXCLUSION

Escludi dall'invio.

SINTASSI:

```
[get] | restore exclusion
add | remove exclusion <exclusion>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`exclusion` - Estensione

FROM

Indirizzo e-mail contatto.

SINTASSI:

```
[get] | restore from
set from [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo e-mail

LOGING

Creazione rapporto.

SINTASSI:

[get] | restore loging

set loging disabled | enabled

OPERAZIONI:

get - Ripristina impostazione/stato corrente

set - Configura valore/stato

restore - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

disabled - Disattiva la funzione/disattiva la configurazione

enabled - Attiva la funzione/attiva la configurazione

SENDING

Invio di file sospetti.

SINTASSI:

```
[get] | restore sending
```

```
set sending none | ask | auto
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non inviare statistiche

`ask` - Conferma prima dell'invio per l'analisi

`auto` - Invia per l'analisi senza conferma

VIA

Strumento dell'invio file.

SINTASSI:

```
[get] | restore via
```

```
set via auto | ra | direct
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`auto` - Tramite Remote Administrator o direttamente a ESET

`ra` - Tramite Remote Administrator

`direct` - Direttamente a ESET

WHEN

Condizioni di invio dei file sospetti.

SINTASSI:

```
[get] | restore when

set when asap | update
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`asap` - Prima possibile

`update` - Durante l'aggiornamento

4.10.2.73 Contesto - GENERAL TS.NET STATISTICS

SENDING

Invio di informazioni statistiche.

SINTASSI:

```
[get] | restore sending

set sending disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

WHEN

Invio di informazioni statistiche anonime.

SINTASSI:

```
[get] | restore when

set when asap | update
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`asap` - Prima possibile

`update` - Durante l'aggiornamento

4.10.2.74 Contesto - SCANNER

CLEANLEVEL

Livello di pulitura.

SINTASSI:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Non pulire

`normal` - Pulitura standard

`strict` - Massima pulitura

EXTENSIONS

Estensioni controllate/escluse.

SINTASSI:

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`extension` - Estensione

`all` - Tutti i file

`extless` - File senza estensione

PROFILE

Gestione profili di controllo del computer.

SINTASSI:

```
[get] profile
```

```
select | remove profile <name>
```

`add profile new: <name> [copyfrom: <name>]`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`select` - Seleziona voce

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`name` - Nome profilo

`new` - Nuovo profilo

`copyfrom` - Copia impostazioni da profilo

NOTA: altri comandi contestuali fanno riferimento al profilo attivo (contrassegnato con - x). Per selezionare il profilo attivo, utilizzare `select scanner profile <profile name>`.

SCAN

Controllo del computer.

SINTASSI:

`[get] | clear scan`

`start scan [readonly]`

`pause | resume | stop scan <ID> | all`

OPERAZIONI:

`get` - Mostra controlli in esecuzione e completati

`start` - Esegui controllo computer per profilo selezionato

`stop` - Interrompi controllo

`resume` - Continua il controllo sospeso

`pause` - Sospendi controllo

`clear` - Rimuovi controlli completati dall'elenco

ARGOMENTI:

`readonly` - Controllo senza rimozione

`ID` - ID controllo per l'esecuzione del comando

`all` - Esegui comando per tutti i controlli

TARGET

Oggetti da controllare per il profilo attivo.

SINTASSI:

`[get] target`

`add | remove target <path>`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`path` - Percorso/oggetti da controllare

NOTA: per il controllo del settore di avvio, immettere `X:\${Boot}` dove 'X' è il nome dell'unità controllata.

4.10.2.75 Contesto - SCANNER LIMITS ARCHIVE

LEVEL

Livello di ricerca negli archivi.

SINTASSI:

```
[get] | restore level

set level <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Livello da 1 a 20 oppure 0 per le impostazioni predefinite

SIZE

Dimensione massima file in archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

4.10.2.76 Contesto - SCANNER LIMITS OBJECTS

SIZE

Dimensione massima dell'archivio (kB).

SINTASSI:

```
[get] | restore size

set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione in kB oppure 0 per le impostazioni predefinite

TIMEOUT

Tempo massimo del controllo per gli archivi (sec.).

SINTASSI:

```
[get] | restore timeout

set timeout <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Tempo in secondi oppure O per le impostazioni predefinite

4.10.2.77 Contesto - SCANNER OBJECTS

ARCHIVE

Controlla archivi.

SINTASSI:

```
[get] | restore archive

set archive disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

BOOT

Controlla settori di avvio.

SINTASSI:

```
[get] | restore boot

set boot disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

EMAIL

Controlla file e-mail.

SINTASSI:

```
[get] | restore email

set email disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

MEMORY

Controlla memoria.

SINTASSI:

```
[get] | restore memory

set memory disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

RUNTIME

Controlla eseguibili compressi.

SINTASSI:

```
[get] | restore runtime

set runtime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SFX

Controlla archivi autoestraenti.

SINTASSI:

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.78 Contesto - SCANNER OPTIONS

ADVHEURISTICS

Utilizza euristica avanzata.

SINTASSI:

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HEURISTICS

Utilizza euristica.

SINTASSI:

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNSAFE

Rilevamento delle applicazioni potenzialmente pericolose.

SINTASSI:

```
[get] | restore unsafe
```

```
set unsafe disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

UNWANTED

Rilevamento delle applicazioni potenzialmente indesiderate.

SINTASSI:

```
[get] | restore unwanted
set unwanted disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.79 Contesto - SCANNER OTHER

ADS

Controllo alternate data streams (ADS).

SINTASSI:

```
[get] | restore ads
set ads disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

LOGALL

Registra tutti gli oggetti.

SINTASSI:

```
[get] | restore logall
set logall disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

LOWPRIORITY

Esegui controlli in background con priorità bassa.

SINTASSI:

```
[get] | restore lowpriority
```

```
set lowpriority disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

OPTIMIZE

Ottimizzazione Smart.

SINTASSI:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

PRESERVETIME

Mantieni timestamp ultimo accesso.

SINTASSI:

```
[get] | restore preservetime
```

```
set preservetime disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SCROLL

Scorri rapporto del controllo.

SINTASSI:

```
[get] | restore scroll
```

```
set scroll disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.80 Contesto - SERVER

AUTOEXCLUSIONS

Gestione esclusioni automatiche.

SINTASSI:

```
[get] | restore autoexclusions
```

```
select autoexclusions <server>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`select` - Seleziona voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`server` - Nome del server

4.10.2.81 Contesto - TOOLS

QUARANTINE

Quarantena.

SINTASSI:

```
[get] quarantine
```

```
add quarantine <path>
```

```
send | remove | restore quarantine <ID>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

`send` - Invia voce/file

ARGOMENTI:

`path` - Percorso file

`ID` - ID file in quarantena

STATISTICS

Statistiche.

SINTASSI:

```
[get] | clear statistics
```

OPERAZIONI:

`get` - Visualizza statistiche

`clear` - Azzera statistiche

SYSINSPECTOR

SysInspector.

SINTASSI:

```
[get] sysinspector
```

```
add | remove sysinspector <name>
```

```
export sysinspector <name> to:<path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`export` - Esporta in un file

ARGOMENTI:

`name` - Commento

`path` - Nome del file (ZIP o XML)

4.10.2.82 Contesto - TOOLS ACTIVITY

FILESYSTEM

Attività del file system.

SINTASSI:

```
[get] filesystem [<count>] [seconds | minutes | hours [<year>-<month>]]
```

ARGOMENTI:

`count` - Numero di record da visualizzare

`seconds` - Campionamento di 1 secondo

`minutes` - Campionamento di 1 minuto

`hours` - Campionamento di 1 ora

`year` - Anno da visualizzare

`month` - Mese da visualizzare

4.10.2.83 Contesto - TOOLS LOG

DETECTIONS

Risulta utile per visualizzare le informazioni sulle infiltrazioni rilevate.

PERCORSO CONTESTUALE:

```
root
```

SINTASSI:

```
[get] detections [count <number>] [from <year>-<month>-<day> <hour>:<minute>:<second>] [to <year>-<month>-<day> <hour>
```

```
clear detections
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`clear` - Rimuove tutti gli elementi/file

ARGOMENTI:

`count` - Mostra numero selezionato di record

`number` - Numero di record

`from` - Visualizza record dall'ora specificata

`year` - Anno

`month` - Mese

`day` - Giorno

`hour` - Ora

`minute` - Minuti

`second` - Secondi

`to` - Visualizza record fino l'ora specificata

ALIAS:

```
virlog
```

ESEMPI:

`get detections from 2011-04-14 01:30:00` - Visualizza tutte le infiltrazioni rilevate dopo il 14 aprile 2011 01:30:00 (per il corretto funzionamento del comando, quando si definisce la data è necessario includere anche l'ora)

`clear detections` - Cancella l'intero rapporto

EVENTS

Risulta utile per visualizzare le informazioni su vari eventi.

SINTASSI:

```
[get] events [count <number>] [from <year>-<month>-<day> <hour>:<minute>:<second>] [to <year>-<month>-<day>
<hour>:<minute>:<second>]
```

```
clear events
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`clear` - Rimuove tutti gli elementi/file

ARGOMENTI:

`count` - Mostra numero selezionato di record

`number` - Numero di record

`from` - Visualizza record dall'ora specificata

`year` - Anno

`month` - Mese

`day` - Giorno

`hour` - Ora

`minute` - Minuti

`second` - Secondi

`to` - Visualizza record fino l'ora specificata

ALIAS:

`warnlog`

ESEMPI:

`get events from 2011-04-14 01:30:00` - Visualizza tutti gli eventi che si sono verificati dopo il 14 aprile 2011 01:30:00 (per il corretto funzionamento del comando, quando si definisce la data è necessario includere anche l'ora)

`clear events` - Cancella l'intero rapporto

FILTER

Livello di dettaglio minimo degli eventi da visualizzare.

SINTASSI:

```
[get] | restore filter
```

```
set filter [[none] [critical] [errors] [warnings] [informative] [diagnostic] [all]] [smart]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - Nessun record

`critical` - Errori critici

`errors` - Errori

`warnings` - Avvisi

`informative` - Record informativi

`diagnostic` - Record di diagnostica

`all` - Tutti i record

`smart` - Filtraggio smart

SCANS

Rapporto 'controllo computer' o elenco rapporti.

SINTASSI:

```
[get] scans [id:<id>] [count:<number>] [from:<year>-<month>-<day> <hour>:<minute>:<second>] [to:<year>-<month>-
```

```
<day> <hour>:<minute>:<second>]
clear scans
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`clear` - Rimuove tutti gli elementi/file

ARGOMENTI:

`id` - Visualizza dettagli del controllo computer con ID

`id` - ID controllo

`count` - Mostra solo numero selezionato di record

`number` - Numero di record

`from` - Visualizza solo record dall'ora specificata

`year` - Anno

`month` - Mese

`day` - Giorno

`hour` - Ora

`minute` - Minuti

`second` - Secondi

`to` - Visualizza solo record dall'ora specificata

VERBOSITY

Livello minimo di dettaglio del rapporto.

SINTASSI:

```
[get] | restore verbosity
set verbosity critical | errors | warnings | informative | diagnostic
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`critical` - Errori critici

`errors` - Errori

`warnings` - Avvisi

`informative` - Record informativi

`diagnostic` - Record di diagnostica

4.10.2.84 Contesto - TOOLS LOG CLEANING

TIMEOUT

Durata record file di rapporto (giorni).

SINTASSI:

```
[get] | restore timeout
```

```
set timeout <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Giorni (1 - 365)

USE

Eliminazione automatica dei rapporti.

SINTASSI:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.85 Contesto - TOOLS LOG OPTIMIZE

LEVEL

Ottimizzazione superando il numero di record non usati (percentuale).

SINTASSI:

```
[get] | restore level
```

```
set level <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Percentuale di record non usati (1 - 100)

NOW

Ottimizza immediatamente file di protocollo.

SINTASSI:

```
now
```

L'esecuzione del comando potrebbe richiedere alcuni minuti.

USE

Ottimizzazione automatica dei rapporti.

SINTASSI:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.86 Contesto - TOOLS NOTIFICATION

VERBOSITY

Livello di dettaglio minimo per le notifiche.

SINTASSI:

```
[get] | restore verbosity
```

```
set verbosity critical | errors | warnings | informative | diagnostic
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`critical` - Errori critici

`errors` - Errori

`warnings` - Avvisi

`informative` - Record informativi

`diagnostic` - Record di diagnostica

4.10.2.87 Contesto - TOOLS NOTIFICATION EMAIL

FROM

Indirizzo e-mail del mittente.

SINTASSI:

```
[get] | restore from

set from [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo e-mail

LOGIN

Nome accesso.

SINTASSI:

```
[get] | restore login

set login [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome

PASSWORD

Password.

SINTASSI:

```
[get] | restore password

set password [plain <password>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

SERVER

Indirizzo server SMTP.

SINTASSI:

```
[get] | restore server
```

```
set server [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo

TO

Indirizzo e-mail del destinatario.

SINTASSI:

```
[get] | restore to
```

```
set to [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo e-mail

USE

Invio di eventi tramite e-mail.

SINTASSI:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.88 Contesto - TOOLS NOTIFICATION MESSAGE ENCODING

Codifica dei messaggi di avviso.

SINTASSI:

```
[get] | restore encoding

set encoding nolocal | localcharset | localencoding | ISO-2022-JP
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`nolocal` - Non utilizzare caratteri alfabetici nazionali

`localcharset` - Utilizza caratteri alfabetici nazionali

`localencoding` - Utilizza caratteri alfabetici nazionali e codifica

`ISO` - Utilizza la codifica ISO-2022-JP (solo per la versione giapponese)

4.10.2.89 Contesto - TOOLS NOTIFICATION MESSAGE FORMAT DETECTION

Formato dei messaggi di avviso per le minacce.

SINTASSI:

```
[get] | restore detection

set detection [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Formato dei messaggi

Opzioni dei formati dei messaggi:

`%TimeStamp%` - Data e ora dell'evento

`%Scanner%` - Modulo che ha rilevato l'evento

`%ComputerName%` - Nome del computer

`%ProgramName%` - Programma che ha causato l'evento

`%ErrorDescription%` - Descrizione dell'errore

Per il formato dei messaggi è necessario sostituire le parole chiave (visualizzate in questo caso con il segno percentuale "%") con i valori corrispondenti.

NOTA: il formato dei messaggi e degli avvisi virus di ESET File Security è predefinito e non è consigliabile modificarlo. È possibile modificare il formato nel caso in cui si utilizzi un sistema automatico di gestione dei messaggi e-mail.

EVENT

Formato degli eventi.

SINTASSI:

```
[get] | restore event

set event [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Formato dei messaggi

Opzioni dei formati dei messaggi:

`%TimeStamp%` - Data e ora dell'evento

`%Scanner%` - Modulo che ha rilevato l'evento

`%ComputerName%` - Nome del computer

`%ProgramName%` - Programma che ha causato l'evento

`%InfectedObject%` - Oggetto infetto (file, e-mail, ecc.)

`%VirusName%` - Nome del virus

Per il formato dei messaggi è necessario sostituire le parole chiave (visualizzate in questo caso con il segno percentuale "%") con i valori corrispondenti.

NOTA: il formato dei messaggi e degli avvisi virus di ESET File Security è predefinito e non è consigliabile modificarlo. È possibile modificare il formato nel caso in cui si utilizzi un sistema automatico di gestione dei messaggi e-mail.

4.10.2.90 Contesto - TOOLS NOTIFICATION WINPOPUP

ADDRESS

Invia notifiche ai nomi computer.

SINTASSI:

```
[get] | restore address

set address [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome computer delimitato da virgole

TIMEOUT

Intervallo di invio ai computer LAN.

SINTASSI:

```
[get] | restore timeout
```

`set timeout <number>`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Intervallo in secondi (1 - 3600)

USE

Invia eventi ai computer LAN.

SINTASSI:

`[get] | restore use`

`set use disabled | enabled`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.91 Contesto - TOOLS SCHEDULER

AZIONE

Azione attività pianificata.

SINTASSI:

`[get] action`

`set action external | logmaintenance | startupcheck | status | scan | update`

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`external` - Esegui applicazione esterna

`logmaintenance` - Manutenzione rapporto

`startupcheck` - Controllo all'avvio

`status` - Crea snapshot di stato computer

`scan` - Controllo del computer

`update` - Aggiornamento

TASK

Attività pianificata.

SINTASSI:

```
[get] | select task [<ID>]
set task <ID> disabled | enabled
add task <task_name>
remove | start task <ID>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`select` - Seleziona voce

`add` - Aggiunge voce

`remove` - Rimuove voce

`start` - Inizia attività

ARGOMENTI:

`ID` - ID attività

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

`task_name` - Nome dell'attività

TRIGGER

Esecuzione attività.

SINTASSI:

```
[get] trigger
set trigger once | repeat | daily | weekly | event
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`once` - Una volta

`repeat` - Ripetutamente

`daily` - Ogni giorno

`weekly` - Ogni settimana

`event` - Quando si verifica un evento

4.10.2.92 Contesto - TOOLS SCHEDULER EVENT

INTERVAL

Esegui l'attività solo una volta entro l'intervallo specificato (ore).

SINTASSI:

```
[get] interval
set interval <hours>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`hours` - Tempo in ore (1 - 720 ore)

TYPE

Attività attivata da un evento.

SINTASSI:

```
[get] type
```

```
set type startup | startuponcedaily | dialup | engineupdate | appupdate | logon | detection
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`startup` - All'avvio del computer

`startuponcedaily` - Al primo avvio del computer ogni giorno

`dialup` - Connessione remota a Internet/VPN

`engineupdate` - Aggiornamento del database delle firme antivirali

`appupdate` - Aggiornamento dei componenti di programma

`logon` - All'accesso utente

`detection` - Rilevamento delle minacce

4.10.2.93 Contesto - TOOLS SCHEDULER FAILSAFE

EXECUTE

Azione da eseguire se l'attività non viene eseguita.

SINTASSI:

```
[get] execute
```

```
set execute asap | iftimeout | no
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`asap` - Esegui l'attività appena possibile

`iftimeout` - E&segui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato

`no` - Non eseguire con ritardo

NOTA: per configurare un limite, immettere `SET TOOLS SCHEDULER EDIT FAILSAFE TIMEOUT <HOURS>`.

TIMEOUT

Intervallo attività (ore).

SINTASSI:

```
[get] timeout
```

```
set timeout <hours>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`hours` - Tempo in ore (1 - 720 ore)

4.10.2.94 Contesto - TOOLS SCHEDULER PARAMETERS CHECK

LEVEL

Livello di controllo.

SINTASSI:

```
[get] level
```

```
set level [before_logon | after_logon | most_frequent | frequent | common | rare | all]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`before_logon` - File eseguiti prima dell'accesso utente

`after_logon` - File eseguiti dopo l'accesso utente

`most_frequent` - Solo i file utilizzati più di frequente

`frequent` - File utilizzati di frequente

`common` - File utilizzati comunemente

`rare` - File utilizzati raramente

`all` - File registrati

PRIORITY

Priorità di controllo.

SINTASSI:

```
[get] priority
```

```
set priority [normal | low | lowest | idle]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`normal` - Normale

`low` - Bassa

`lowest` - Più bassa

`idle` - Quando inattivo

4.10.2.95 Contesto - TOOLS SCHEDULER PARAMETERS EXTERNAL

ARGUMENTS

Argomenti.

SINTASSI:

```
[get] arguments
```

```
set arguments <arguments>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`arguments` - Argomenti

DIRECTORY

Cartella di lavoro.

SINTASSI:

```
[get] directory
```

```
set directory <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`path` - Percorso

EXECUTABLE

File eseguibile.

SINTASSI:

```
[get] executable
```

```
set executable <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`path` - Percorso

4.10.2.96 Contesto - TOOLS SCHEDULER PARAMETERS SCAN

PROFILE

Profilo di controllo.

SINTASSI:

```
[get] profile
```

```
set profile <profile>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`profile` - Nome profilo

READONLY

Controllo senza rimozione.

SINTASSI:

```
[get] readonly
```

```
set readonly disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

TARGET

Oggetti da controllare.

SINTASSI:

```
[get] | clear target
```

```
add | remove target <path>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`add` - Aggiunge voce

`remove` - Rimuove voce

`clear` - Rimuove tutti gli elementi/file

ARGOMENTI:

`path` - Oggetti da controllare/percorso

4.10.2.97 Contesto - TOOLS SCHEDULER PARAMETERS UPDATE

PRIMARY

Profilo di aggiornamento.

SINTASSI:

```
[get] primary
```

```
set primary [<profile>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`profile` - Nome profilo

SECONDARY

Profilo di aggiornamento alternativo.

SINTASSI:

```
[get] secondary
```

```
set secondary [<profile>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`profile` - Nome profilo

4.10.2.98 Contesto - TOOLS SCHEDULER REPEAT

INTERVAL

Intervallo dell'attività (minuti).

SINTASSI:

```
[get] interval
```

```
set interval <minutes>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`minutes` - Tempo in minuti (1 - 720 ore)

4.10.2.99 Contesto - TOOLS SCHEDULER STARTUP

DATE

L'attività verrà eseguita alla data selezionata.

SINTASSI:

```
[get] date
```

```
set date <year>-<month>-<day>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`year` - Anno

`month` - Mese

`day` - Giorno

DAYS

Esegui l'attività nei giorni seguenti.

SINTASSI:

```
[get] days
```

```
set | add | remove days none | [monday] [tuesday] [wednesday] [thurdsday] [friday] [saturday] [sunday] | all
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`none` - Nessun giorno specificato

`monday` - Lunedì

`tuesday` - Martedì

`wednesday` - Mercoledì

`thurdsday` - Giovedì

`friday` - Venerdì

`saturday` - Sabato

`sunday` - Domenica

`all` - Ogni giorno

TIME

L'attività verrà eseguita all'ora selezionata.

SINTASSI:

```
[get] time
```

```
set time <hour>:<minute>:<second>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

ARGOMENTI:

`hour` - Ora

`minute` - Minuti

`second` - Secondi

4.10.2.100 Contesto - UPDATE

CACHE

Cancella la cache dell'aggiornamento.

SINTASSI:

```
clear cache
```

COMPONENTS

Aggiorna componenti di programma.

SINTASSI:

```
[get] | restore components
```

```
set components never | allways | ask
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`never` - Non aggiornare

`allways` - Aggiorna sempre

`ask` - Chiedi prima di scaricare i componenti di programma

LOGIN

Nome utente dell'accesso.

SINTASSI:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome

NOTA: immettere il nome utente e la password ricevuti dopo l'acquisto o la registrazione È consigliabile copiarli (CTRL+C) dall'e-mail di registrazione e incollarli (CTRL+V).

PASSWORD

Password.

SINTASSI:

```
[get] | restore password

set password [plain <password>]
```

OPERAZIONI:

`get` - Mostra password

`set` - Imposta o cancella password

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

NOTA: immettere il nome utente e la password ricevuti dopo l'acquisto o la registrazione È consigliabile copiarli (CTRL+C) dall'e-mail di registrazione e incollarli (CTRL+V).

PRERELEASE

Attiva aggiornamenti pre-rilascio.

SINTASSI:

```
[get] | restore prerelease

set prerelease disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

PROFILE

Gestione profili di aggiornamento.

SINTASSI:

```
[get] profile

select | remove profile <name>

add profile new: <name> [copyfrom: <name>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`select` - Seleziona voce

`add` - Aggiunge voce

`remove` - Rimuove voce

ARGOMENTI:

`name` - Nome profilo

`new` - Nuovo profilo

`copyfrom` - Copia impostazione da profilo

NOTA: altri comandi contestuali fanno riferimento al profilo attivo (contrassegnato con - x). Per selezionare il profilo attivo, utilizzare `seleziona scanner profilo <nome profilo>`.

SERVER

Server di aggiornamento.

SINTASSI:

```
[get] | restore server
```

```
select | add | remove server <server>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`select` - Seleziona voce

`add` - Aggiunge voce

`remove` - Rimuove voce

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`server` - Indirizzo server

STATUS

Visualizza stato dell'aggiornamento.

SINTASSI:

```
[get] status
```

UPDATE

Aggiornamento.

SINTASSI:

```
start | stop update
```

OPERAZIONI:

`start` - Esegui aggiornamento

`stop` - Annulla aggiornamento

4.10.2.101 Contesto - UPDATE CONNECTION

DISCONNECT

Disconnetti dal server dopo l'aggiornamento.

SINTASSI:

```
[get] | restore disconnect
```

```
set disconnect disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

LOGIN

Nome utente.

SINTASSI:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome

PASSWORD

Password.

SINTASSI:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERAZIONI:

`get` - Mostra password

`set` - Imposta o cancella password

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

RUNAS

Connetti a LAN come.

SINTASSI:

```
[get] | restore runas
```

```
set runas system | current | specified
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`system` - Account di sistema (predefinito)

`current` - Utente corrente

`specified` - Utente specificato

4.10.2.102 Contesto - UPDATE MIRROR

COMPONENTS

Aggiorna componenti di programma.

SINTASSI:

```
[get] | start | restore components
```

```
set components disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`start` - Avvia aggiornamento

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

CARTELLA

Cartella per l'archiviazione dei file con mirroring.

SINTASSI:

```
[get] | restore folder
```

```
set folder [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Percorso della cartella

LOGIN

Nome utente.

SINTASSI:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome

PASSWORD

Password.

SINTASSI:

```
[get] | restore password

set password [plain <password>]
```

OPERAZIONI:

`get` - Mostra password

`set` - Imposta o cancella password

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

USE

Crea mirror di aggiornamento.

SINTASSI:

```
[get] | restore use

set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

VERSIONS

Gestione versioni di aggiornamento.

SINTASSI:

```
[get] | restore versions

select versions <version>
```

OPERAZIONI:

`get` - Visualizza versioni disponibili

`select` - Seleziona/deseleziona versione di aggiornamento

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`version` - Nome della versione

4.10.2.103 Contesto - UPDATE MIRROR CONNECTION

DISCONNECT

Disconnetti dal server dopo l'aggiornamento.

SINTASSI:

```
[get] | restore disconnect
```

```
set disconnect disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

LOGIN

Nome utente.

SINTASSI:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome

PASSWORD

Password.

SINTASSI:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERAZIONI:

`get` - Mostra password

`set` - Imposta o cancella password

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

RUNAS

Connetti a LAN come.

SINTASSI:

```
[get] | restore runas
```

```
set runas system | current | specified
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`system` - Account di sistema (predefinito)

`current` - Utente corrente

`specified` - Utente specificato

4.10.2.104 Contesto - UPDATE MIRROR SERVER

AUTHENTICATION

Utilizza autenticazione.

SINTASSI:

```
[get] | restore authentication
```

```
set authentication none | basic | ntlm
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`none` - No

`basic` - Standard

`ntlm` - NTLM

PORT

Porta.

SINTASSI:

```
[get] | restore port
```

```
set port <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Numero di porta.

USE

Fornisci i file di aggiornamento tramite il server HTTP interno.

SINTASSI:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

4.10.2.105 Contesto - UPDATE NOTIFICATION

DOWNLOAD

Chiedi prima di scaricare l'aggiornamento.

SINTASSI:

```
[get] | restore download
```

```
set download disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

HIDE

Non visualizzare notifiche relative agli aggiornamenti riusciti.

SINTASSI:

```
[get] | restore hide
```

```
set hide disabled | enabled
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`disabled` - Disattiva la funzione/disattiva la configurazione

`enabled` - Attiva la funzione/attiva la configurazione

SIZE

Chiedi se un file di aggiornamento è maggiore di (kB).

SINTASSI:

```
[get] | restore size
```

```
set size <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Dimensione file (kB)

NOTA: per disattivare le notifiche di aggiornamento immettere `0`.

4.10.2.106 Contesto - UPDATE PROXY

LOGIN

Nome utente.

SINTASSI:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Nome

MODE

Configurazione proxy HTTP.

SINTASSI:

```
[get] | restore mode
```

```
set mode global | noproxy | userdefined
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`global` - Utilizza impostazioni server proxy globali

`noproxy` - Non utilizzare server proxy

`userdefined` - Connessione tramite server proxy

PASSWORD

Password.

SINTASSI:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERAZIONI:

`get` - Mostra password

`set` - Imposta o cancella password

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`plain` - Opzione per immettere la password come parametro

`password` - Password

PORT

Porta del server proxy.

SINTASSI:

```
[get] | restore port
```

```
set port <number>
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`number` - Numero di porta.

SERVER

Server proxy.

SINTASSI:

```
[get] | restore server
```

```
set server [<string>]
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`string` - Indirizzo server

4.10.2.107 Contesto - UPDATE SYSTEM

NOTIFY

Notifica gli aggiornamenti mancanti a partire dal livello.

SINTASSI:

```
[get] | restore notify
```

```
set notify no | optional | recommended | important | critical
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`no` - No

`optional` - Opzionale

`recommended` - Consigliato

`important` - Importante

`critical` - Critico

RESTART

Riavvia il computer al termine dell'aggiornamento dei componenti di programma.

SINTASSI:

```
[get] | restore restart

set restart never | ask | auto
```

OPERAZIONI:

`get` - Ripristina impostazione/stato corrente

`set` - Configura valore/stato

`restore` - Ripristina impostazioni predefinite/oggetto/file

ARGOMENTI:

`never` - Non riavviare

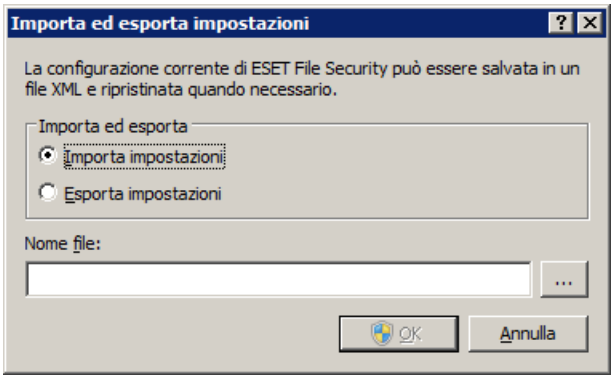
`ask` - Chiedi prima di riavviare

`auto` - Riavvia automaticamente

4.11 Importa ed esporta impostazioni

La funzione di importazione ed esportazione delle configurazioni di ESET File Security è disponibile in **Configurazione** facendo clic su **Importa ed esporta impostazioni**.

Le opzioni di importazione e di esportazione utilizzano entrambe il tipo di file XML. Le opzioni di importazione e di esportazione sono utili nel caso in cui si desideri effettuare il backup della configurazione corrente di ESET File Security per poterlo utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per quegli utenti che desiderano utilizzare la configurazione preferita di ESET File Security su più sistemi. In tal modo, sarà infatti possibile importare facilmente un file XML per il trasferimento delle impostazioni desiderate.



4.12 ThreatSense.Net

Il Sistema di allarme immediato ThreatSense.Net mantiene ESET tempestivamente e periodicamente informato sulle nuove infiltrazioni. Lo scopo del Sistema di allarme immediato ThreatSense.Net bidirezionale è unicamente quello di migliorare la protezione offerta. Il modo migliore per assicurare il rilevamento di nuove minacce non appena appaiono consiste nell'"essere collegati" al maggior numero possibile di clienti e di utilizzarli come rilevatori di minacce. Sono disponibili due opzioni:

1. È possibile decidere di non abilitare il Sistema di allarme immediato ThreatSense.Net. Non verranno perse funzionalità del software, che continuerà ad offrire la migliore protezione in assoluto.

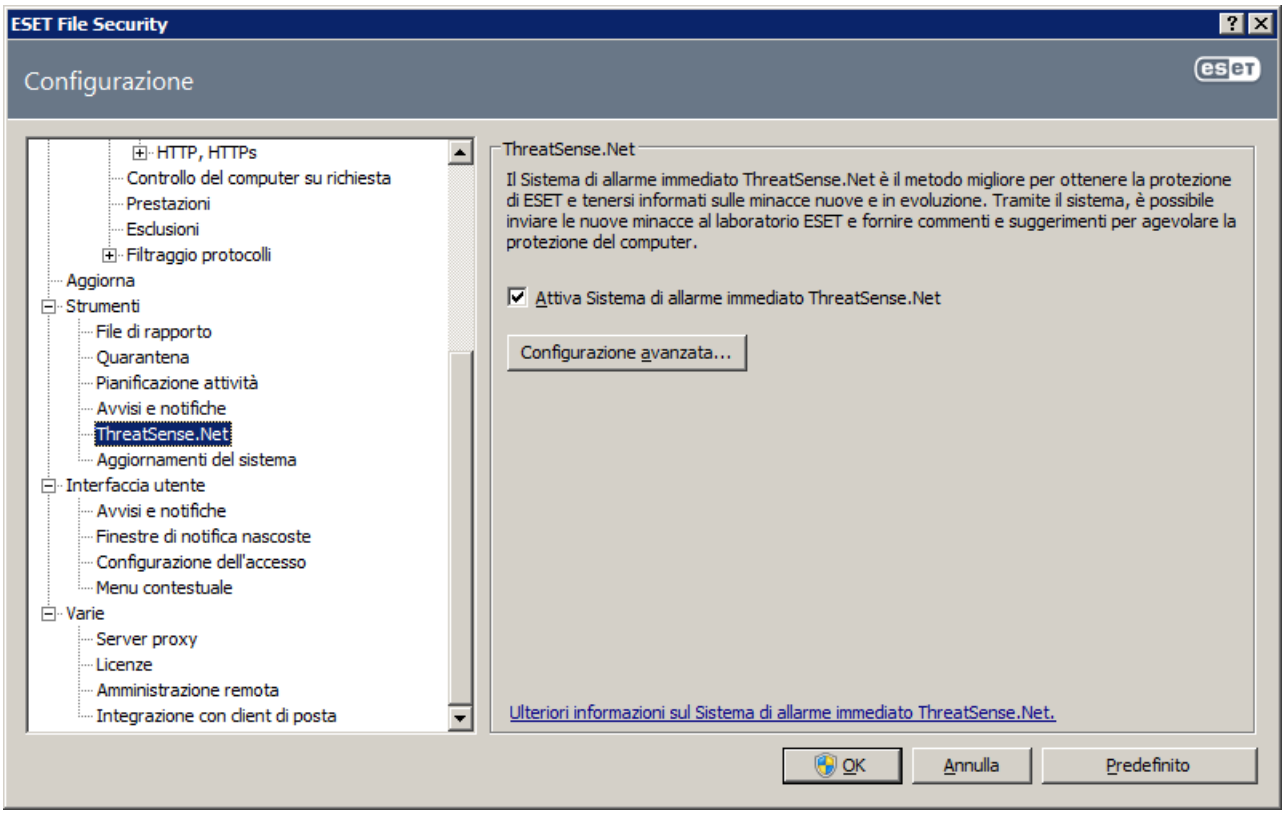
2. È possibile configurare il Sistema di allarme immediato ThreatSense.Net per l'invio di informazioni anonime sulle nuove minacce e laddove sia presente il nuovo codice dannoso. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà utile a ESET per aggiornare le proprie capacità di rilevamento.

Il Sistema di allarme immediato ThreatSense.Net raccoglierà informazioni sul computer degli utenti in relazione alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso al file, il nome del file, informazioni su data e ora, il processo in base al quale la minaccia è apparsa sul computer e informazioni sul sistema operativo del computer.

Sebbene esista la possibilità che vengano trasmesse occasionalmente informazioni sull'utente o sul computer (nomi utenti nel percorso di una directory e così via) ai laboratori antivirus ESET, tali informazioni saranno utilizzate ESCLUSIVAMENTE allo scopo di rispondere in modo immediato alle nuove minacce.

Per impostazione predefinita, ESET File Security è configurato per richiedere conferma prima di inviare file sospetti per l'analisi dettagliata ai laboratori antivirus ESET. Sono sempre esclusi file con determinate estensioni, ad esempio DOC o XLS. È inoltre possibile aggiungere altre estensioni qualora sussistano specifici file che l'utente o la società dell'utente non desidera inviare.

È possibile accedere alla configurazione di ThreatSense.Net dalla struttura Configurazione avanzata in **Strumenti** > **ThreatSense.Net**. Selezionare l'opzione **Attiva Sistema di allarme immediato ThreatSense** per attivarlo, quindi fare clic sul pulsante **Configurazione avanzata...**.

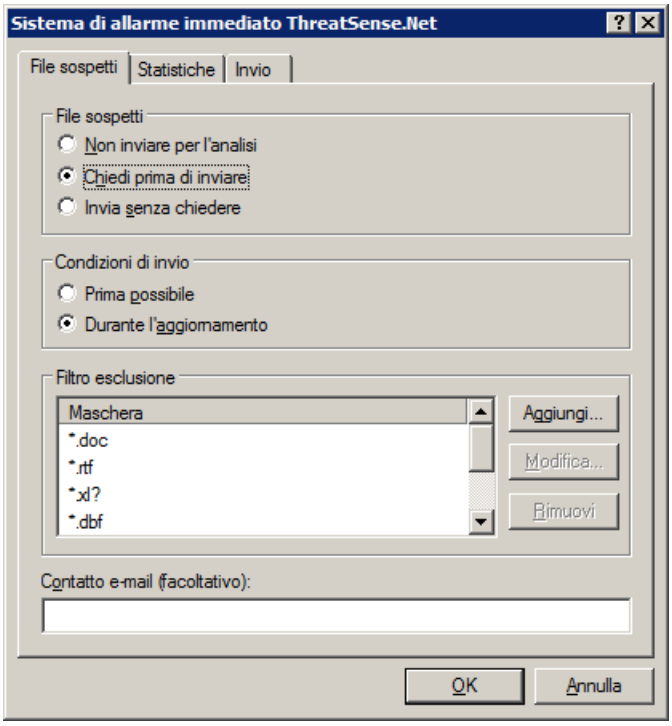


4.12.1 File sospetti

La scheda **File sospetti** consente di configurare il modo in cui le minacce vengono inviate ai laboratori antivirus ESET.

Se si rileva un file sospetto, è possibile inviarlo per l'analisi ai ThreatLabs. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento delle firme antivirali.

È possibile impostare l'invio automatico dei file, oppure selezionare l'opzione **Chiedi prima di inviare** se si desidera sapere quali file sono stati inviati per l'analisi e confermarne l'invio.



Se non si desidera inviare alcun file, selezionare l'opzione **Non inviare per l'analisi**. La scelta di non inviare i file per l'analisi non influenza l'invio delle informazioni statistiche configurate nella rispettiva impostazione (consultare la sezione Statistiche).

Condizioni di invio - Per impostazione predefinita, è selezionata l'opzione **Prima possibile** per l'invio dei file sospetti ai laboratori antivirus ESET. Questa opzione è consigliata se è disponibile una connessione Internet permanente e i file sospetti possono essere inviati immediatamente. Selezionare l'opzione **Durante l'aggiornamento** per caricare i file sospetti su ThreatSense.Net nel corso del successivo aggiornamento.

Filtro di esclusione - Il Filtro di esclusione consente di escludere dall'invio determinati file/cartelle. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (con estensione DOC e così via). È possibile aggiungerli alla lista degli elementi esclusi dal controllo.

Contatto e-mail (facoltativo) - Il **Contatto e-mail [facoltativo]** può essere inviato insieme ai file sospetti e potrebbe essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

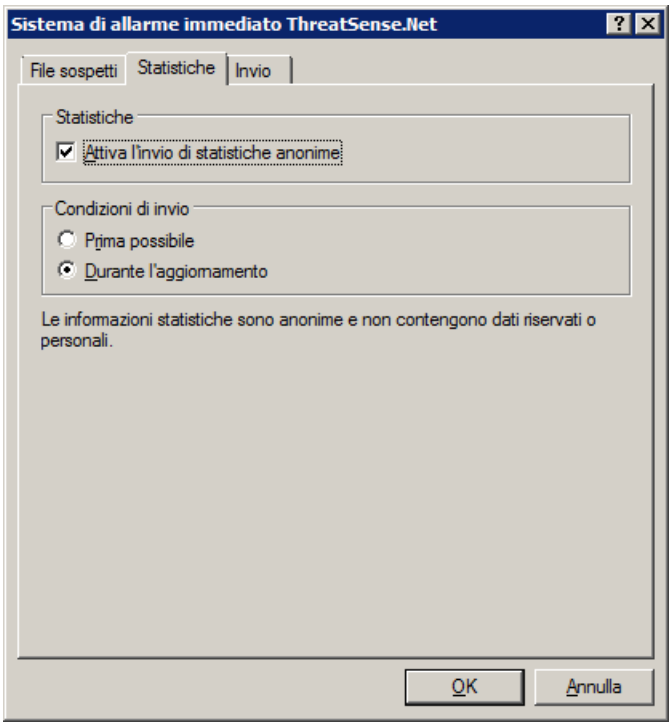
4.12.2 Statistiche

Il Sistema di allarme immediato ThreatSense.Net raccoglierà informazioni anonime sul computer degli utenti in relazione alle nuove minacce rilevate. Queste informazioni possono includere il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione del prodotto di protezione ESET, la versione del sistema operativo in uso e le impostazioni di ubicazione. Di norma, le statistiche vengono inviate ai server di ESET una o due volte al giorno.

Di seguito viene riportato un esempio di pacchetto statistico inviato:

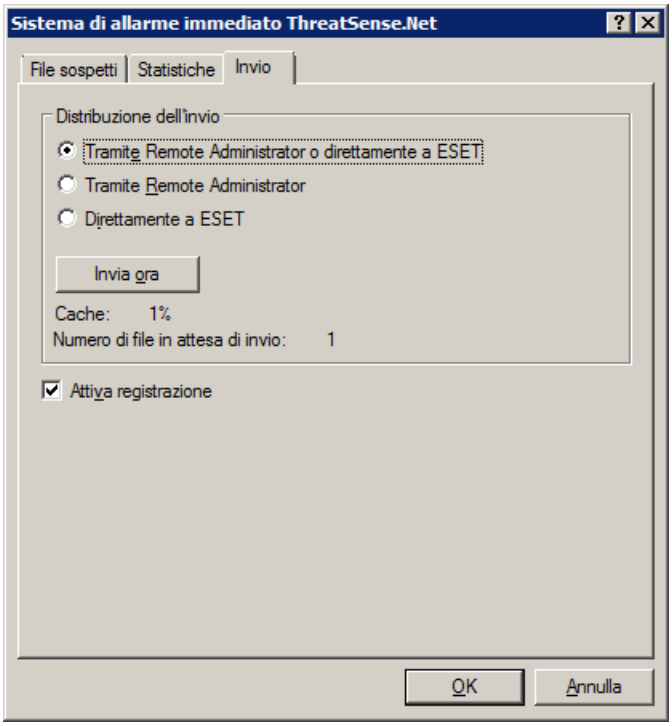
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

Condizioni di invio - È possibile decidere quando inviare le informazioni statistiche. Se si sceglie l'opzione **Prima possibile**, le informazioni statistiche verranno inviate non appena vengono create. Questa impostazione è adatta se è disponibile una connessione Internet permanente. Se l'opzione **Durante l'aggiornamento** è selezionata, tutte le informazioni statistiche verranno inviate nel corso del successivo aggiornamento.



4.12.3 Invio

È possibile decidere le modalità di invio a ESET dei file e delle informazioni statistiche. Selezionare l'opzione **Tramite Remote Administrator o direttamente a ESET** per inviare i file e le statistiche mediante tutti i mezzi disponibili. Selezionare l'opzione **Tramite Remote Administrator** per inviare i file e le statistiche al server di amministrazione remota, garantendo così il successivo invio ai laboratori antivirus ESET. Se si seleziona l'opzione **Direttamente a ESET**, tutti i file sospetti e le informazioni statistiche vengono inviati ai laboratori antivirus ESET direttamente dal programma.



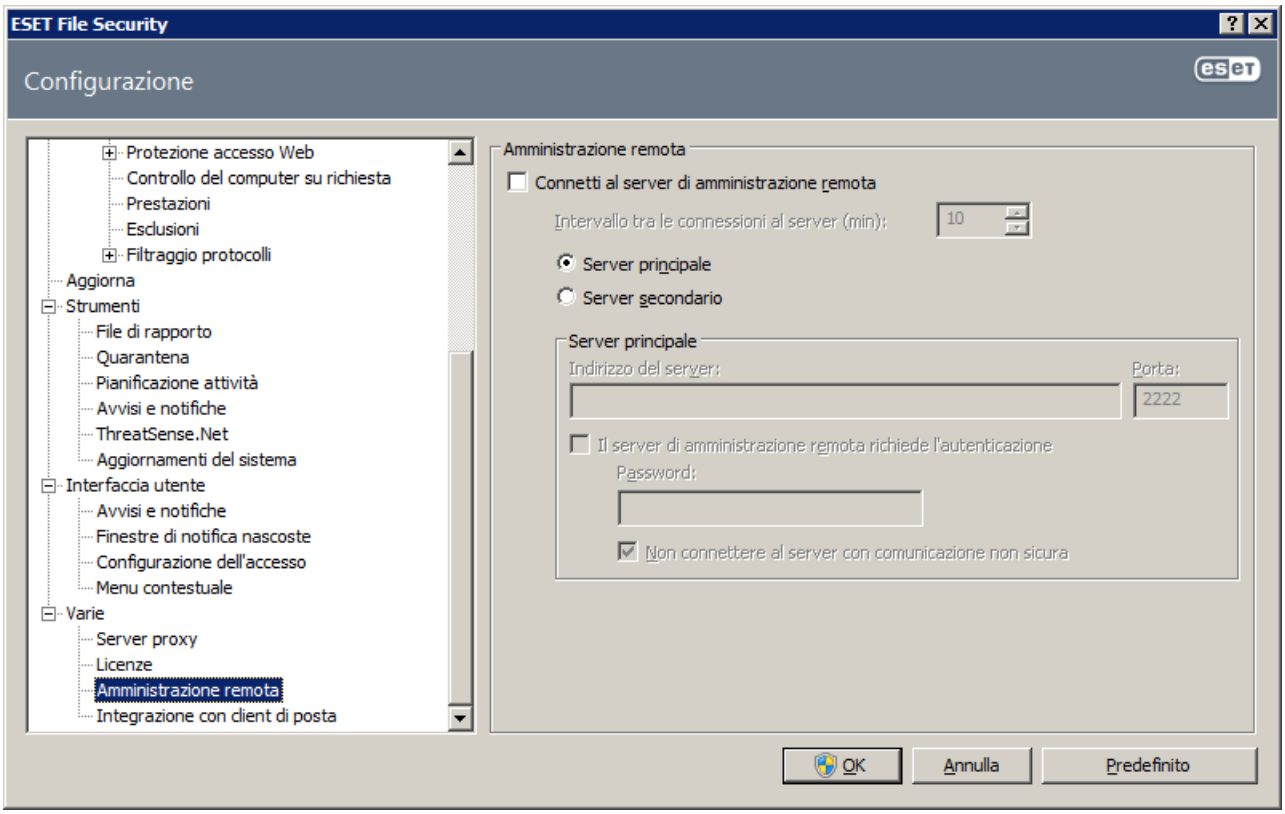
In presenza di file in attesa di invio, il pulsante **Invia ora** sarà attivo. Selezionare questo pulsante per inviare immediatamente i file e le informazioni statistiche.

Selezionare l'opzione **Attiva registrazione** per creare un rapporto sul quale sono registrati gli invii dei file e delle informazioni statistiche.

4.13 Amministrazione remota

ESET Remote Administrator (ERA) è un utile strumento utilizzato per la gestione del sistema di sicurezza e per ottenere una panoramica della sicurezza globale all'interno di una rete. È particolarmente utile quando si applica a reti di una certa dimensione. ERA non solo consente di migliorare i livelli di sicurezza, ma garantisce anche una facilità di utilizzo nella gestione di ESET File Security sulle workstation client.

Le opzioni di configurazione dell'amministrazione remota sono disponibili nella schermata principale di ESET File Security. Fare clic su **Configurazione** > **Immetti struttura di configurazione avanzata completa...** > **Varie** > **Amministrazione remota**.



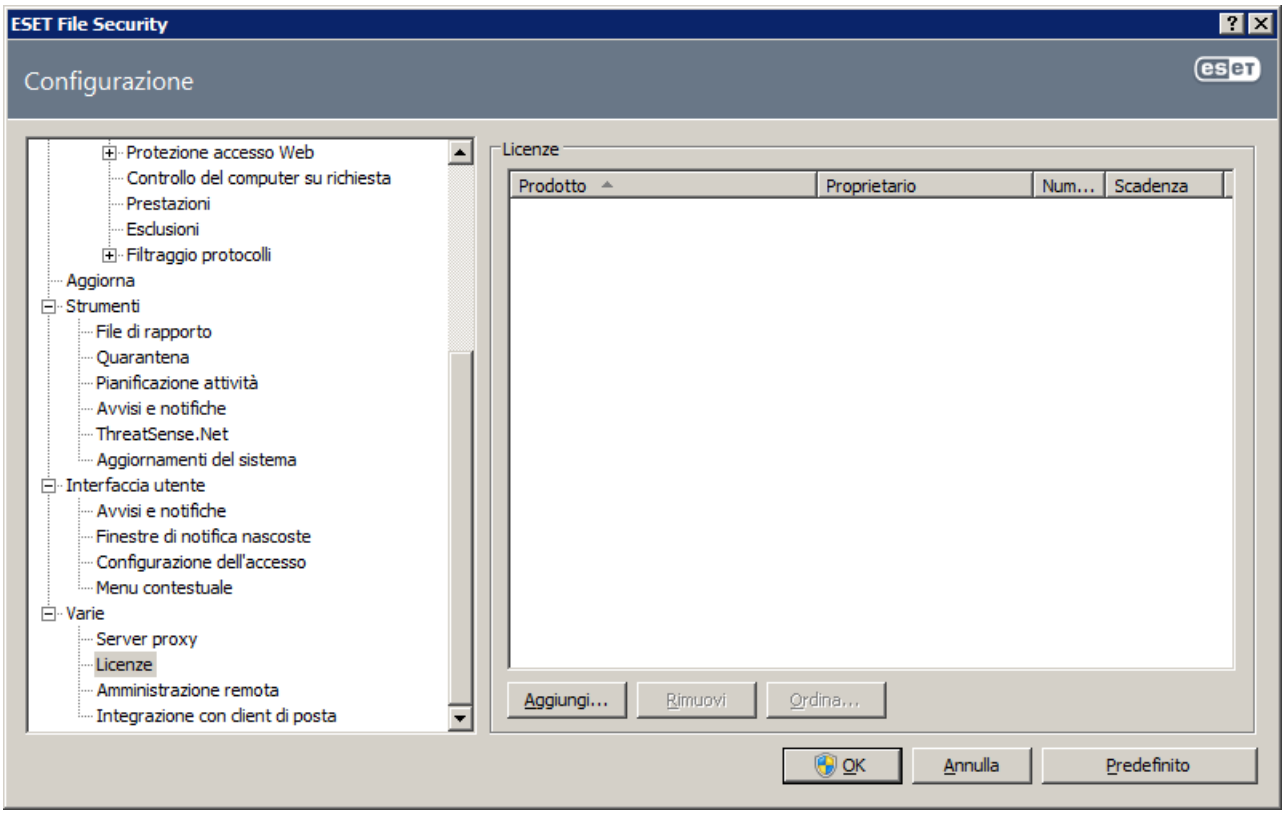
Attivare l'amministrazione remota selezionando l'opzione **Connetti al server di amministrazione remota**. È possibile quindi accedere alle altre opzioni descritte di seguito:

- **Intervallo tra le connessioni al server (min):** Indica la frequenza con la quale ESET File Security si connetterà a ERA Server. Se il valore impostato è 0, le informazioni vengono inviate ogni 5 secondi.
- **Indirizzo server:** Indirizzo di rete del server sul quale è installato ERA Server.
- **Porta:** Questo campo contiene la porta server predefinita utilizzata per la connessione. È consigliabile conservare l'impostazione predefinita della porta su 2222.
- **Il server di amministrazione remota richiede l'autenticazione:** Consente di immettere una password per connettersi a ERA Server, se richiesto.

Fare clic su **OK** per confermare le modifiche e applicare le impostazioni. ESET File Security utilizzerà tali impostazioni per connettersi a ERA Server.

4.14 Licenze

Nella sezione **Licenze** è possibile gestire le chiavi di licenza per ESET File Security e altri prodotti ESET, ad esempio ESET Mail Security e così via. Dopo l'acquisito, le chiavi di licenza vengono fornite insieme al nome utente e alla password. Per aggiungere o rimuovere una chiave di licenza, fare clic sul pulsante **Aggiungi/Rimuovi** corrispondente della finestra di gestione licenze. È possibile accedere alla gestione licenze dalla struttura Configurazione avanzata in **Varie** > **Licenze**.



La chiave di licenza è un file di testo contenente informazioni sul prodotto acquistato: il proprietario, il numero di licenze e la data di scadenza.

Nella finestra di gestione delle licenze è possibile caricare e visualizzare il contenuto di una chiave di licenza utilizzando il pulsante **Aggiungi...**. Le informazioni contenute vengono visualizzate nella finestra. Per eliminare i file di licenza dall'elenco, fare clic su **Rimuovi**.

Se una chiave di licenza è scaduta e si desidera rinnovarla, fare clic sul pulsante **Ordina...**. Si verrà reindirizzati al negozio online.

5. Glossario

5.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

5.1.1 Virus

Un virus è un'infiltrazione che danneggia i file presenti sul computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili e i documenti. Per replicarsi, un virus allega se stesso all'interno di un file di destinazione. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

È importante tenere presente che i virus (se paragonati a trojan o spyware) sono sempre più rari, poiché non sono commercialmente allettanti per gli autori di software dannosi. Inoltre, il termine "virus" è spesso utilizzato in modo errato per indicare tutti i tipi di infiltrazioni. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare lo stato originale dei file infetti, ovvero pulirli utilizzando un programma antivirus.

Tra i virus più noti si segnalano: OneHalf, Tenga e Yankee Doodle.

5.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e di viaggiare autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

Tra i worm più noti si segnalano: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

5.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di infiltrazioni che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Tuttavia, è importante notare che ciò era veritiero in passato ma oggi tali programmi non hanno più la necessità di cammuffarsi. Il loro unico scopo è quello di infiltrarsi il più facilmente possibile e portare a termine i loro obiettivi dannosi. Il termine "Trojan horse" ("cavallo di Troia") ha assunto un'accezione molto generale che indica un'infiltrazione che non rientra in una classe specifica di infiltrazioni.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader** - Un programma dannoso in grado di scaricare altre infiltrazioni da Internet
- **Dropper** - Un tipo di trojan horse concepito per installare sui computer compromessi altri tipi di malware
- **Backdoor** - Un'applicazione che comunica con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso a un sistema e assumerne il controllo
- **Keylogger** - (registratore delle battute dei tasti) - Un programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti
- **Dialer** - I dialer sono programmi progettati per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti che è stata creata una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Solitamente, i trojan horse assumono la forma di file eseguibili con estensione .exe. Se sul computer in uso viene rilevato un file classificato come trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

Tra i trojan più noti si segnalano: NetBus, Trojandownloader. Small.ZL, Slapper

5.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevate dal software antivirus: nascondono i processi, i file e i dati del Registro di sistema di Windows. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1) Quando tentano di accedere a un sistema. Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2) Quando sono nascosti dal normale testing. Gli utenti di ESET File Security hanno il vantaggio di poter utilizzare la tecnologia Anti-Stealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

5.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi che visualizzano materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenente pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, sono molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo risiede nel fatto che l'adware può svolgere anche funzioni di rilevamento e registrazione, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non vengono installati senza adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha

dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

5.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

5.1.7 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET File Security offre la possibilità di rilevare tali minacce.

"Applicazioni potenzialmente pericolose" è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

5.1.8 Applicazioni potenzialmente indesiderate

Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- Aperture di nuove finestre mai visualizzate in precedenza
- Attivazione ed esecuzione di processi nascosti
- Maggiore utilizzo delle risorse del sistema
- Modifiche dei risultati di ricerca
- Applicazioni che comunicano con server remoti